

ASDM Book 3: Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide, 7.18

First Published: 2023-09-07

Last Modified: 2019-06-28

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

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

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

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

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

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

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

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

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

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

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

About This Guide xi

Document Objectives xi

Related Documentation xi

Document Conventions xi

Communications, Services, and Additional Information xiii

CHAPTER 1

VPN Wizards 1

VPN Overview 1

IPsec Site-to-Site VPN Wizard 2

AnyConnect Client VPN Wizard 4

IPsec IKEv1 Remote Access Wizard 6

IPsec IKEv2 Remote Access Wizard 10

CHAPTER 2

IKE 13

Configure IKE 13

Enable IKE 13

IKE Parameters for Site-to-Site VPN 14

About IKEv2 Multi-Peer Crypto Map 17

Guidelines for IKEv2 Multi-Peer 19

IKE Policies 20

Add or Edit an IKEv1 Policy 21

Add or Edit an IKEv2 Policy 22

Configure IPsec 24

Crypto Maps 25

Create or Edit an IPsec Rule Tunnel Policy (Crypto Map) - Basic Tab 27

Create or Edit IPsec Rule Tunnel Policy (Crypto Map) - Advanced Tab 29

Create or Edit IPsec Rule Traffic Selection Tab 30
IPsec Pre-Fragmentation Policies 33
Configure IKEv2 Fragmentation Options 34
IPsec Proposals (Transform Sets) 35

CHAPTER 3 **High Availability Options 39**
High Availability Options 39
VPN and Clustering on the Secure Firewall eXtensible Operating System (FXOS) Chassis 39
VPN Load Balancing 40
Failover 40
VPN Load Balancing 40
About VPN Load Balancing 40
VPN Load-Balancing Algorithm 41
VPN Load-Balancing Group Configurations 42
VPN Load Balancing Director Election 42
Frequently Asked Questions About VPN Load Balancing 43
Licensing for VPN Load Balancing 44
Prerequisites for VPN Load Balancing 45
Guidelines and Limitations for VPN Load Balancing 45
Configuring VPN Load Balancing 47
Configure VPN Load Balancing with the High Availability and Scalability Wizard 47
Configure VPN Load Balancing (Without the Wizard) 48
Feature History for VPN Load Balancing 50

CHAPTER 4 **General VPN Setup 51**
System Options 51
Configure Maximum VPN Sessions 53
Configure DTLS 53
Configure DNS Server Groups 54
Configure the Pool of Cryptographic Cores 55
Client Addressing for SSL VPN Connections 55
Group Policies 56
External Group Policies 58
Password Management with AAA Servers 59

Internal Group Policies 60
Internal Group Policy, General Attributes 60
Configure Internal Group Policy, Server Attributes 63
Internal Group Policy, Browser Proxy 64
AnyConnect Client Internal Group Policies 65
Internal Group Policy, Advanced, AnyConnect Client 65
Configure Split-Tunneling for AnyConnect Client Traffic 68
Configure Dynamic Split Tunneling 71
Configure Dynamic Split Exclude Tunneling 71
Configure Dynamic Split Include Tunneling 72
Configure the Management VPN Tunnel 73
Configure Linux to Support Excluded Subnets 74
Internal Group Policy, AnyConnect Client Attributes 74
Internal Group Policy, AnyConnect Client Login Settings 77
Using Client Firewall to Enable Local Device Support for VPN 77
Internal Group Policy, AnyConnect Client Key Regeneration 81
Internal Group Policy, AnyConnect Client, Dead Peer Detection 82
Internal Group Policy, AnyConnect Client Customization of Clientless Portal 83
Configure AnyConnect Client Custom Attributes in an Internal Group Policy 83
IPsec (IKEv1) Client Internal Group Policies 84
Internal Group Policy, General Attributes for IPsec (IKEv1) Client 84
About Access Rules for IPsec (IKEv1) Client in an Internal Group Policy 85
Internal Group Policy, Client Firewall for IPsec (IKEv1) Client 86
Site-to-Site Internal Group Policies 88
Configure VPN Policy Attributes for a Local User 89
Connection Profiles 91
AnyConnect Client Connection Profile, Main Pane 91
Specify a Device Certificate 93
Connection Profiles, Port Settings 93
AnyConnect Client Connection Profile, Basic Attributes 94
Connection Profile, Advanced Attributes 96
AnyConnect Client Connection Profile, General Attributes 97
Connection Profile, Client Addressing 97
Connection Profile, Client Addressing, Add or Edit 99

Connection Profile, Address Pools 99
Connection Profile, Advanced, Add or Edit IP Pool 99
AnyConnect Client Connection Profile, Authentication Attributes 99
Connection Profile, Secondary Authentication Attributes 101
AnyConnect Client Connection Profile, Authorization Attributes 104
AnyConnect Client Connection Profile, Authorization, Add Script Content to Select Username 105
Connection Profiles, Accounting 107
Connection Profile, Group Alias and Group URL 108
IKEv1 Connection Profiles 108
IPsec Remote Access Connection Profile, Basic Tab 109
Add/Edit Remote Access Connections, Advanced, General 109
IKEv1 Client Addressing 111
IKEv1 Connection Profile, Authentication 111
IKEv1 Connection Profile, Authorization 111
IKEv1 Connection Profile, Accounting 111
IKEv1 Connection Profile, IPsec 111
IKEv1 Connection Profile, IPsec, IKE Authentication 112
IKEv1 Connection Profile, IPsec, Client Software Update 112
IKEv1 Connection Profile, PPP 113
IKEv2 Connection Profiles 113
IPsec IKEv2 Connection Profile, Basic Tab 114
IPsec Remote Access Connection Profile, Advanced, IPsec Tab 115
Mapping Certificates to IPsec or SSL VPN Connection Profiles 115
Certificate to Connection Profile Maps, Policy 115
Certificate to Connection Profile Maps Rules 116
Certificate to Connection Profile Maps, add Certificate Matching Rule Criterion 116
Add/Edit Certificate Matching Rule Criterion 117
Site-to-Site Connection Profiles 119
Add or Edit Site-to-Site Connection Profile 119
Site-to-Site Tunnel Groups 121
Site-to-Site Connection Profile, Crypto Map Entry 123
Managing CA Certificates 124
Site-to-Site Connection Profile, Install Certificate 125
AnyConnect VPN module of Cisco Secure Client Image 125

AnyConnect Client External Browser SAML Package 126
Configure AnyConnect Client VPN Connections 128
Guidelines and Limitations for AnyConnect Client Connections 128
Configure AnyConnect Client Profiles 128
Exempt AnyConnect Client Traffic from Network Address Translation 129
AnyConnect Client HostScan 135
Prerequisites for HostScan/Secure Firewall Posture 135
Licensing for AnyConnect Client HostScan/Secure Firewall Posture 135
HostScan Packaging 135
Install or Upgrade HostScan/Secure Firewall Posture 135
Configure Posture Settings 136
Uninstall HostScan/Secure Firewall Posture 137
Assign AnyConnect Client Feature Modules to Group Policies 137
HostScan/Secure Firewall Posture Related Documentation 139
Secure Client Solution 139
Add or Edit MUS Access Control 141
AnyConnect Client Customization and Localization 141
AnyConnect Client Customization and Localization, Resources 141
AnyConnect Client Customization and Localization, Binary and Script 142
AnyConnect Client Customization and Localization, GUI Text and Messages 143
AnyConnect Client Customization and Localization, Customized Installer Transforms 143
AnyConnect Client Customization and Localization, Localized Installer Transforms 143
AnyConnect Client Custom Attributes 143
IPsec VPN Client Software 146
Zone Labs Integrity Server 146
ISE Policy Enforcement 147
Configure ISE Change of Authorization 147

CHAPTER 5 **IP Addresses for VPNs** 151
Configure an IP Address Assignment Policy 151
Configure IP Address Assignment Options 152
View Address Assignment Methods 153
Configure Local IP Address Pools 153
Configure Local IPv4 Address Pools 153

Configure Local IPv6 Address Pools 154
Assign Internal Address Pools to Group Policies 154
Configure DHCP Addressing 155
Assign IP Addresses to Local Users 156

CHAPTER 6 **Dynamic Access Policies 159**
About Dynamic Access Policies 159
DAP Support of Remote Access Protocols and Posture Assessment Tools 160
Remote Access Connection Sequence with DAPs 160
Licensing for Dynamic Access Policies 161
Configure Dynamic Access Policies 161
Add or Edit a Dynamic Access Policy 163
Import and Export the DAP XML File between Two ASAs 164
Test Dynamic Access Policies 165
Configure AAA Attribute Selection Criteria in a DAP 165
Retrieve Active Directory Groups 167
AAA Attribute Definitions 168
Configure Endpoint Attribute Selection Criteria in a DAP 168
Add an Anti-Malware Endpoint Attribute to a DAP 170
Add an Application Attribute to a DAP 170
Add AnyConnect Client Endpoint Attributes to a DAP 171
Add a File Endpoint Attribute to a DAP 172
Add a Device Endpoint Attribute to a DAP 173
Add a NAC Endpoint Attribute to a DAP 173
Add an Operating System Endpoint Attribute to a DAP 174
Add a Personal Firewall Endpoint Attribute to a DAP 174
Add a Policy Endpoint Attribute to a DAP 175
Add a Process Endpoint Attribute to a DAP 175
Add a Registry Endpoint Attribute to a DAP 175
Add Multiple Certificate Authentication Attributes to DAP 176
DAP and Antimalware and Personal Firewall Programs 176
Endpoint Attribute Definitions 177
Create Additional DAP Selection Criteria in DAP Using LUA 180
Syntax for Creating LUA EVAL Expressions 181

LUA Procedures for HostScan 4.6 (and Later) and Secure Firewall Posture Version 5 181
LUA Script for 'ANY' Antimalware (endpoint.am) with Last Update 181
LUA Script for 'ANY' Personal Firewall 182
Additional LUA Functions 182
Examples of DAP EVAL Expressions 184
Configure DAP Access and Authorization Policy Attributes 186
Configure SAML Authorization Using DAP 190
Perform a DAP Trace 191
Examples of DAPs 192
Use DAP to Define Network Resources 192
Use DAP to Apply a WebVPN ACL 193
Enforce CSD Checks and Apply Policies via DAP 193
Use DAP to Check Session Token Security 194

CHAPTER 7 **Email Proxy** 197
Configure Email Proxy 198
Requirements for Email Proxy 198
Set AAA Server Groups 198
Identify Interfaces for Email Proxy 199
Configure Authentication for Email Proxy 200
Identify Proxy Servers 201
Configure Delimiters 202

CHAPTER 8 **Monitor VPN** 203
Monitor VPN Connection Graphs 203
Monitor VPN Statistics 203

CHAPTER 9 **SSL Settings** 209
SSL Settings 209

CHAPTER 10 **Virtual Tunnel Interface** 213
About Virtual Tunnel Interfaces 213
Guidelines for Virtual Tunnel Interfaces 213
Create a VTI Tunnel 215

Add an IPsec Proposal (Transform Sets) 216
Add an IPsec Profile 217
Add a VTI Interface 218
Feature History for Virtual Tunnel Interface 220

CHAPTER 11 **Configure an External AAA Server for VPN** 223
About External AAA Servers 223
Understanding Policy Enforcement of Authorization Attributes 223
Guidelines For Using External AAA Servers 224
Configure Multiple Certificate Authentication 224
Active Directory/LDAP VPN Remote Access Authorization Examples 225
Policy Enforcement of User-Based Attributes 225
Enforce Static IP Address Assignment for AnyConnect Client Tunnels 227
Enforce Dial-in Allow or Deny Access 228
Enforce Logon Hours and Time-of-Day Rules 231



About This Guide

The following topics explain how to use this guide.

- Document Objectives, on page xi
- Related Documentation, on page xi
- Document Conventions, on page xi
- Communications, Services, and Additional Information, on page xiii

Document Objectives

The purpose of this guide is to help you configure VPN on the Secure Firewall ASA using the Adaptive Security Device Manager (ASDM), a web based GUI application. This guide does not cover every feature, but describes only the most common configuration scenarios.

This guide applies to the ASA series. Throughout this guide, the term "ASA" applies generically to supported models, unless specified otherwise.

Related Documentation

For more information, see *Navigating the Cisco ASA Series Documentation* at http://www.cisco.com/go/asadocs.

Document Conventions

This document adheres to the following text, display, and alert conventions.

Text Conventions

Convention	Indication
boldface	Commands, keywords, button labels, field names, and user-entered text appear in **boldface**. For menu-based commands, the full path to the command is shown.
italic	Variables, for which you supply values, are presented in an *italic* typeface. Italic type is also used for document titles, and for general emphasis.

Convention	Indication
`monospace`	Terminal sessions and information that the system displays appear in `monospace` type.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in square brackets and separated by vertical bars.
[ ]	Default responses to system prompts are also in square brackets.
< >	Non-printing characters such as passwords are in angle brackets.
!, #	An exclamation point (!) or a number sign (#) at the beginning of a line of code indicates a comment line.

Reader Alerts

This document uses the following for reader alerts:



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Tip Means *the following information will help you solve a problem.*



Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.



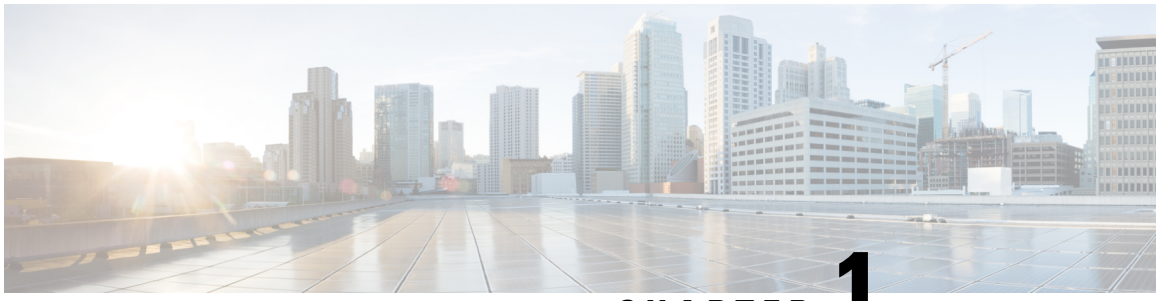
Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

VPN Wizards

- VPN Overview, on page 1
- IPsec Site-to-Site VPN Wizard, on page 2
- **AnyConnect Client VPN Wizard**, on page 4
- IPsec IKEv1 Remote Access Wizard, on page 6
- IPsec IKEv2 Remote Access Wizard, on page 10

VPN Overview

The ASA creates a Virtual Private Network by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

The secure connection is called a tunnel, and the ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

The VPN wizard lets you configure basic LAN-to-LAN and remote access VPN connections and assign either preshared keys or digital certificates for authentication. Use ASDM to edit and configure advanced features.

The four VPN wizards described in this section are as follows:

- AnyConnect Client VPN Wizard, on page 4

  The Cisco AnyConnect VPN client provides secure SSL or IPsec (IKEv2) connections to the ASA for remote users with full VPN tunneling to corporate resources. Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept clientless VPN connections. The ASA downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure connection and either remains or uninstalls itself (depending on the ASA configuration) when the connection terminates. In the case of a previously installed client, when the user authenticates, the ASA examines the revision of the client and upgrades the client as necessary.

  The AnyConnect Client VPN wizard will be available only in the User Contexts when ASA is in multi-context mode. The Storage and Resource Class for the required context must be configured from the System Context.

Storage per context is required to have Cisco AnyConnect Client Package and Profile files. Resource Class is required for license allotment for each context. The license utilized is AnyConnect Client Premium.



Note The rest of the configuration for this wizard remains the same as single-context.

- IPsec IKEv2 Remote Access Wizard, on page 10

IKEv2 allows other vendors' VPN clients to connect to the ASAs. This enhances security and complies with the IPsec remote access requirements defined in federal and public sector mandates.

The IPSec IKEv2 Remote Access wizard will be available only in the User Contexts when ASA is in multi-context mode. Resource Class for the required context must be configured from the System Context for license allotment. The license utilized is the AnyConnect Client Premium.



Note The rest of the configuration for this wizard remains the same as single-context.

- IPsec IKEv1 Remote Access Wizard, on page 6
- IPsec Site-to-Site VPN Wizard, on page 2

For LAN-to-LAN connections using both IPv4 and IPv6 addressing, the ASA supports VPN tunnels if both peers are ASAs, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6). This is also true if both peer inside networks are IPv6 and the outside network is IPv6.

IPsec Site-to-Site VPN Wizard

A tunnel between two ASA devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Peer Device Identification

- Peer IP Address—Configure the IP address of the other site (peer device).
- VPN Access Interface—Select the interface to use for the site-to-site tunnel.
- Crypto Map Type—Specify the type of maps that will be used for this peer, static or dynamic.

Traffic to Protect

This step lets you identify the local network and remote network These networks protect the traffic using IPsec encryption.

- Local Networks—Identify the host used in the IPsec tunnel.
- Remote Networks—Identify the networks used in the IPsec tunnel.

Security

This step lets you configure the methods to authenticate with the peer device. You can either choose the simple configuration, and supply a preshared key. Or you can choose Customized Configuration for more advanced options, as follows:

- IKE Version—Check the IKEv1 or IKEv2 check box according to which version you want to use.
- IKE version 1 Authentication Methods
  - Pre-shared Key—Using a preshared key is a quick and easy way to set up communication with a limited number of remote peers and a stable network. It may cause scalability problems in a large network because each IPsec peer requires configuration information for each peer with which it establishes secure connections.

    Each pair of IPsec peers must exchange preshared keys to establish secure tunnels. Use a secure method to exchange the preshared key with the administrator of the remote site.
  - Device Certificate—Click to use certificates for authentication between the local ASA and the remote IPsec peer.

    You can efficiently manage the security keys used to establish an IPsec tunnel with digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the public key.

    When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA, and none of the other peers require additional configuration.
- IKE version 2 Authentication Methods
  - Local Pre-shared Key—Specify IPsec IKEv2 authentication methods and encryption algorithms.
  - Local Device Certificate—Authenticates VPN access through the security appliance.
  - Remote Peer Pre-shared Key—Enter a preshared key for authentication between the local ASA and the remote IPsec peer.
  - Remote Peer Certificate Authentication—When checked, the peer device is allowed to use the certificate to authenticate itself to this device.
- Encryption Algorithms—This tab lets you choose the types of encryption algorithms used to protect the data.
  - IKE Policy—Specify IKEv1/IKEv2 authentication methods.
  - IPsec Proposal—Specify IPsec encryption algorithms.
- Perfect Forward Secrecy
  - Enable Perfect Forwarding Secrecy (PFS)—Specify whether to use Perfect Forward Secrecy, and the size of the numbers to use, in generating Phase 2 IPsec keys. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless PFS is enabled. PFS uses Diffie-Hellman techniques to generate the keys.

    PFS ensures that a session key derived from a set of long-term public and private keys is not compromised if one of the private keys is compromised in the future.

PFS must be enabled on both sides of the connection.

- Diffie-Hellman Group—Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default Group 14 (2048 -bit Diffie-Hellman).

NAT Exempt

- Exempt ASA side host/network from address translation—Use the drop-down list to choose a host or network to be excluded from address translation.

AnyConnect Client VPN Wizard

Use this wizard to configure ASA to accept VPN connections from the AnyConnect VPN client. This wizard configures either IPsec (IKEv2) or SSL VPN protocols for full network access. The ASA automatically uploads the AnyConnect VPN client to the end user's device when a VPN connection is established.

Connection Profile Identification

The connection profile identification is used to identify the ASA to the remote acess users:

- Connection Profile Name—Provide a name that the remote access users will access for VPN connections.
- VPN Access Interface—Choose an interface that the remote access users will access for VPN connections.

VPN Protocols

Specify the VPN protocol allowed for this connection profile.

The AnyConnect Client defaults to SSL. If you enable IPsec as a VPN tunnel protocol for the connection profile, you must also create and deploy a client profile with IPsec enabled using the profile editor from ASDM, and deploy the profile.

If you predeploy instead of weblaunch the AnyConnect Client, the first client connection uses SSL, and receives the client profile from the ASA during the session. For subsequent connections, the client uses the protocol specified in the profile, either SSL or IPsec. If you predeploy the profile with IPsec specified with the client, the first client connection uses IPsec. For more information about predeploying a client profile with IPsec enabled, see the *Secure Client Administrator Guide*.

- SSL
- IPsec (IKE v2)
- Device Certificate—Identifies the ASA to the remote access clients. Some AnyConnect Client features (such as always on, IPsec/IKEv2) require a valid device certificate on the ASA.
- Manage—Choosing **Manage** opens the Manage Identity Certificates window.
  - Add—Choose **Add** to add an identity certificate and its details.
  - Show Details—If you choose a particular certificate and click **Show Details**, the Certificate Details window appears and provides who the certificate was issued to and issued by, as well as specifics about its serial number, usage, associated trustpoints, valid timeframe, and so on.

- Delete—Highlight the certificate you want to remove and click **Delete**.
- Export—Highlight the certificate and click **Export** to export the certificate to a file with or without an encryption passphrase.
- Enroll ASA SSL VPN with Entrust—Gets your ASA SSL VPN appliance up and running quickly with an SSL Advantage digital certificate from Entrust.

Client Images

ASA can automatically upload the latest AnyConnect Client package to the client device when it accesses the enterprise network. You can use a regular expression to match the user agent of a browser to an image. You can also minimize connection setup time by moving the most commonly encountered operation system to the top of the list.

Authentication Methods

Specify authentication information on this screen.

- AAA server group—Enable to let the ASA contact a remote AAA server group to authenticate the user. Select a AAA server group from the list of pre-configured groups or click **New** to create a new group.
- Local User Database Details—Add new users to the local database stored on the ASA.
  - Username—Create a username for the user.
  - Password—Create a password for the user.
  - Confirm Password—Re-type the same password to confirm.
  - Add/Delete—Add or delete the user from the local database.

Client Address Assignment

Provide a range of IP addresses to remote AnyConnect Client users.

- IPv4 Address Pools—SSL VPN clients receive new IP addresses when they connect to the ASA. Clientless connections do not require new IP addresses. Address Pools define a range of addresses that remote clients can receive. Select an existing IP Address Pool or click **New** to create a new pool.

  If you choose **New**, you will have to provide a starting and ending IP address and subnet mask.

- IPv6 Address Pool—Select an existing IP Address Pool or click **New** to create a new pool.



Note IPv6 address pools can not be created for IKEv2 connection profiles.

Network Name Resolution Servers

Specify which domain names are resolved for the remote user when accessing the internal network.

- DNS Servers—Enter the IP address of the DNS server.

- WINS Servers—Enter the IP address of the WINS server.
- Domain Name—Type the default domain name.

NAT Exempt

If network translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

AnyConnect Client Deployment

You can install the AnyConnect Client program to a client device using one of the following two methods:

- Web launch—The AnyConnect Client package installs automatically when accessing the ASA using a web browser.

Note Web launch is not supported in multiple-context mode.

- Pre-deployment—Manually install the AnyConnect Client package.

Allow Web Launch is a global setting that affects all connections. If it is unchecked (disallowed), AnyConnect Client SSL connections and clientless SSL connections do not work.

For pre-deployment, the disk0:/test2_client_profile.xml profile bundle contains an .msi file, and you must include this client profile from the ASA in your AnyConnect Client package to ensure IPsec connection functions as expected.

IPsec IKEv1 Remote Access Wizard

Note The Cisco VPN Client is end-of-life and end-of-support. You must upgrade to the Secure Client.

Use the IKEv1 Remote Access Wizard to configure secure remote access for VPN clients, such as mobile users, and to identify the interface that connects to the remote IPsec peer.

- VPN Tunnel Interface—Choose the interface to use for remote access clients. If the ASA has multiple interfaces, stop now and configure the interfaces on the ASA before running this wizard.
- Enable inbound IPsec sessions to bypass interface access lists—Enable IPsec authenticated inbound sessions to always be permitted through the ASA (that is, without checking the interface access-list statements). Be aware that the inbound sessions bypass only the interface ACLs. Configured group-policy, user, and downloaded ACLs still apply.

Remote Access Client

Remote access users of various types can open VPN tunnels to this ASA. Choose the type of VPN client for this tunnel.

- VPN Client Type

- Easy VPN Remote product.
- Microsoft Windows client using L2TP over IPsec—Specify the PPP authentication protocol. The choices are PAP, CHAP, MS-CHAP-V1, MS-CHAP-V2, and EAP-PROXY:

  PAP—Passes the cleartext username and password during authentication and is not secure.

  CHAP—In response to the server challenge, the client returns the encrypted challenge plus password with a cleartext username. This protocol is more secure than PAP, but it does not encrypt data.

  MS-CHAP, Version 1—Similar to CHAP, but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP.

  MS-CHAP, Version 2—Contains security enhancements over MS-CHAP, Version 1.

  EAP-Proxy—Enables EAP which permits the ASA to proxy the PPP authentication process to an external RADIUS authentication server.

  If a protocol is not specified on the remote client, do no specify it.
- Specify if the client will send the tunnel group name as username@tunnelgroup.

VPN Client Authentication Method and Tunnel Group Name

Use the VPN Client Authentication Method and Name pane to configure an authentication method and create a connection policy (tunnel group).

- Authentication Method—The remote site peer authenticates either with a preshared key or a certificate.
  - Pre-shared Key—Click to use a preshared key for authentication between the local ASA and the remote IPsec peer.

    Using a pre-shared key is a quick and easy way to set up communication with a limited number of remote peers and a stable network. It may cause scalability problems in a large network because each IPsec peer requires configuration information for each peer with which it establishes secure connections.

    Each pair of IPsec peers must exchange preshared keys to establish secure tunnels. Use a secure method to exchange the preshared key with the administrator of the remote site.
  - Pre-shared Key—Type an alphanumeric string between 1 and 128 characters.
  - Certificate—Click to use certificates for authentication between the local ASA and the remote IPsec peer. To complete this section, you must have previously enrolled with a CA and downloaded one or more certificates to the ASA.

    You can efficiently manage the security keys used to establish an IPsec tunnel with digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the public key.

    To use digital certificates, each peer enrolls with a certification authority (CA), which is responsible for issuing digital certificates. A CA can be a trusted vendor or a private CA that you establish within an organization.

    When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA, and none of the other peers require additional configuration.

Certificate Signing Algorithm—Displays the algorithm for signing digital certificates, rsa-sig for RSA.

- Tunnel Group Name—Type a name to create the record that contains tunnel connection policies for this IPsec connection. A connection policy can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes. A connection policy that you configure with this VPN wizard specifies an authentication method and uses the ASA Default Group Policy.

Client Authentication

Use the Client Authentication pane to choose the method by which the ASA authenticates remote users. Select one of the following options:

- Authenticate using the local user database—Click to use authentication internal to the ASA. Use this method for environments with a small, stable number of users. The next pane lets you create accounts on the ASA for individual users.
- Authenticate using an AAA server group—Click to use an external server group for remote user authentication.
  - AAA Server Group Name—Choose a AAA server group configured previously.
  - New...—Click to configure a new AAA server group.

User Accounts

Use the User Accounts pane to add new users to the ASA internal user database for authentication purposes.

Address Pool

Use the Address Pool pane to configure a pool of local IP addresses that the ASA assigns to remote VPN clients.

- Tunnel Group Name—Displays the name of the connection profile (tunnel group) to which this address pool applies. You set this name in the VPN Client and Authentication Method pane (step 3).
- Pool Name—Select a descriptive identifier for the address pool.
- New...—Click to configure a new address pool.
- Range Start Address—Type the starting IP address in the address pool.
- Range End Address—Type the ending IP address in the address pool.
- Subnet Mask—(Optional) Choose the subnet mask for these IP addresses.

Attributes Pushed to Client (Optional)

Use the Attributes Pushed to Client (Optional) pane to have the ASA pass information about DNS and WINS servers and the default domain name to remote access clients.

- Tunnel Group—Displays the name of the connection policy to which the address pool applies. You set this name in the VPN Client Name and Authentication Method pane.
- Primary DNS Server—Type the IP address of the primary DNS server.

- Secondary DNS Server—Type the IP address of the secondary DNS server.
- Primary WINS Server—Type the IP address of the primary WINS server.
- Secondary WINS Server— Type the IP address of the secondary WINS server.
- Default Domain Name—Type the default domain name.

IKE Policy

IKE, also called Internet Security Association and Key Management Protocol (ISAKMP), is the negotiation protocol that lets two hosts agree on how to build an IPsec Security Association. Each IKE negotiation is divided into two sections called Phase1 and Phase 2. Phase 1 creates the first tunnel, which protects later IKE negotiation messages. Phase 2 creates the tunnel that protects data.

Use the IKE Policy pane to set the terms of the Phase 1 IKE negotiations which includes an encryption method to protect the data and ensure privacy, an authentication method to ensure the identity of the peers, and a Diffie-Hellman group to establish the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.

- Encryption—Select the symmetric encryption algorithm the ASA uses to establish the Phase 1 SA that protects Phase 2 negotiations. The ASA supports the following encryption algorithms:

Algorithm	Explanation
DES	Data Encryption Standard. Uses a 56-bit key.
3DES	Triple DES. Performs encryption three times using a 56-bit key.
AES-128	Advanced Encryption Standard. Uses a 128-bit key.
AES-192	AES using a 192-bit key.
AES-256	AES using a 256-bit key.

  The default, 3DES, is more secure than DES but requires more processing for encryption and decryption. Similarly, the AES options provide increased security but also require increased processing.

- Authentication—Choose the hash algorithm used for authentication and ensuring data integrity. The default is SHA. MD5 has a smaller digest and is considered to be slightly faster than SHA. There has been a demonstrated successful (but extremely difficult) attack against MD5. However, the Keyed-Hash Message Authentication Code (HMAC) version used by the ASA prevents this attack.
- Diffie-Hellman Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default DH Group 14 (2048 -bit) is considered as more secure than Group 2 and Group 5.

IPsec Settings (Optional)

Use the IPsec Settings (Optional) pane to identify local hosts/networks which do not require address translation. By default, the ASA hides the real IP addresses of internal hosts and networks from outside hosts by using dynamic or static Network Address Translation (NAT). NAT minimizes risks of attack by untrusted outside hosts but may be improper for those who have been authenticated and protected by VPN.

For example, an inside host using dynamic NAT has its IP address translated by matching it to a randomly selected address from a pool. Only the translated address is visible to the outside. Remote VPN clients that attempt to reach these hosts by sending data to their real IP addresses cannot connect to these hosts, unless you configure a NAT exemption rule.



Note If you want all hosts and networks to be exempt from NAT, configure nothing on this pane. If you have even one entry, all other hosts and networks are subject to NAT.

- Interface—Choose the name of the interface that connects to the hosts or networks you have selected.
- Exempt Networks—Select the IP address of the host or network that you want to exempt from the chosen interface network.
- Enable split tunneling—Select to have traffic from remote access clients destined for the public Internet sent unencrypted. Split tunneling causes traffic for protected networks to be encrypted, while traffic to unprotected networks is unencrypted. When you enable split tunneling, the ASA pushes a list of IP addresses to the remote VPN client after authentication. The remote VPN client encrypts traffic to the IP addresses that are behind the ASA. All other traffic travels unencrypted directly to the Internet without involving the ASA.
- Enable Perfect Forwarding Secrecy (PFS)—Specify whether to use Perfect Forward Secrecy, and the size of the numbers to use, in generating Phase 2 IPsec keys. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless PFS is enabled. PFS uses Diffie-Hellman techniques to generate the keys.

  PFS ensures that a session key derived from a set of long-term public and private keys is not compromised if one of the private keys is compromised in the future.

  PFS must be enabled on both sides of the connection.

  - Diffie-Hellman Group—Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default DH Group 14 (2048 -bit) is considered as more secure than Group 2 and Group 5.

Summary

When you are satisfied with the configuration, click **Finish**. ASDM saves the LAN-to-LAN configuration. After you click **Finish**, you can no longer use the VPN wizard to make changes to this configuration. Use ASDM to edit and configure advanced features.

IPsec IKEv2 Remote Access Wizard

Use the IKEv2 Remote Access Wizard to configure secure remote access for VPN clients, such as mobile users, and to identify the interface that connects to the remote IPsec peer.

Connection Profile Identification

Enter a **Connection Profile Name** and choose the **VPN Access Interface** that will be used for IPsec IKEv2 remote access.

- Connection Profile Name—Type a name to create the record that contains tunnel connection policies for this IPsec connection. A connection policy can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes. A connection policy that you configure with this VPN wizard specifies an authentication method and uses the ASA Default Group Policy.
- VPN Access Interface—Choose the interface that establishes a secure tunnel with the remote IPsec peer. If the ASA has multiple interfaces, you need to plan the VPN configuration before running this wizard, identifying the interface to use for each remote IPsec peer with which you plan to establish a secure connection.

Standards Based IPSec (IKEv2) Authentication Page

IKE Peer Authentication—The remote site peer authenticates either with a preshared key or a certificate or peer authentication using EAP.

- Pre-shared Key—Type an alphanumeric string between 1 and 128 characters.

  Using a pre-shared key is a quick and easy way to set up communication with a limited number of remote peers and a stable network. It may cause scalability problems in a large network because each IPsec peer requires configuration information for each peer with which it establishes secure connections.

  Each pair of IPsec peers must exchange preshared keys to establish secure tunnels. Use a secure method to exchange the preshared key with the administrator of the remote site.

- Enable Certificate Authentication—Allows you to use certificates for authentication if checked.
- Enable peer authentication using EAP—Allows you to use EAP for authentication if checked. You must use certificates for local authentication if you check this check box.
- Send an EAP identity request to the client—Enables you to send an EAP request for authentication to the remote access VPN client.

Mobike RRC

- Enable Return Routability Check for mobike—Enable Return Routability checking for dynamic IP address changes in IKE/IPSEC security associations on which mobike is enabled.

IKE Local Authentication

- Enable local authentication, and select either preshared key or certificate
  - Preshared Key—Type an alphanumeric string between 1 and 128 characters.
  - Certificate—Click to use certificates for authentication between the local ASA and the remote IPsec peer. To complete this section, you must have previously enrolled with a CA and downloaded one or more certificates to the ASA.

    You can efficiently manage the security keys used to establish an IPsec tunnel with digital certificates. A digital certificate contains information that identifies a user or device, such as a name, serial number, company, department or IP address. A digital certificate also contains a copy of the public key.

    To use digital certificates, each peer enrolls with a certification authority (CA), which is responsible for issuing digital certificates. A CA can be a trusted vendor or a private CA that you establish within an organization.

When two peers want to communicate, they exchange certificates and digitally sign data to authenticate each other. When you add a new peer to the network, it enrolls with a CA, and none of the other peers require additional configuration.

Authentication Methods

Only Radius authentication is supported for IPsec IKEv2 remote access.

- AAA Server Group—Choose a AAA server group configured previously.
- New—Click to configure a new AAA server group.
- AAA Server Group Details—Use this area to modify the AAA server group if desired.

Client Address Assignment

Create or select IPv4 and IPv6 address pools. Remote access clients will be assigned addresses from either IPv4 or IPv6 pools. IPv4 addresses take precedence if both are configured. See *Configuring Local IP Address Pools* for more information.

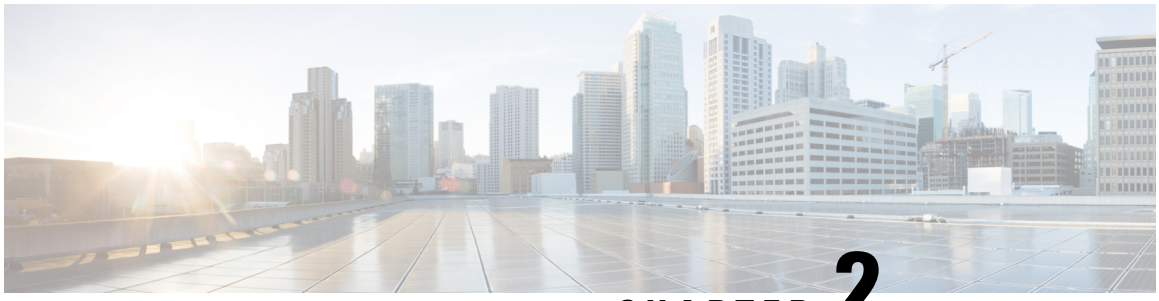
Network Name Resolution Servers

Specify how domain names are resolved for the remote user when accessing the internal network.

- DNS Servers—Type the IP address of the DNS servers.
- WINS Servers—Type the IP address of the WINS servers.
- Default Domain Name—Type the default domain name.

NAT Exempt

- Exempt VPN traffic from Network Address Translation—If NAT is enabled on the ASA this must be checked.



CHAPTER 2

IKE

- Configure IKE, on page 13
- Configure IPsec, on page 24

Configure IKE

IKE, also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. To configure the ASA for Virtual Private Networks, you set global IKE parameters that apply system wide, and you also create IKE policies that the peers negotiate to establish a VPN connection.

Procedure

Step 1 Enable IKE, on page 13.

Step 2 Set IKE Parameters for Site-to-Site VPN, on page 14.

Step 3 Configure IKE Policies, on page 20.

Enable IKE

Procedure

Step 1 To enable IKE for VPN connections:

a) In ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access >AnyConnect Connection Profiles**.

b) In the Access Interfaces area, check **Allow Access** under IPsec (IKEv2) Access for the interfaces you will use IKE on.

Step 2 To enable IKE for Site-to-Site VPN:

a) In ASDM, choose **Configuration > Site-to-Site VPN > Connection Profiles**.

b) Select the interfaces you want to use IKEv1 and IKEv2 on.

IKE Parameters for Site-to-Site VPN

In ASDM, choose **Configuration > Site-to-Site VPN > Advanced > IKE Parameters**.

NAT Transparency

- Enable IPsec over NAT-T

  IPsec over NAT-T lets IPsec peers establish both remote access and LAN-to-LAN connections through a NAT device. It does this by encapsulating IPsec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPsec traffic when necessary. This feature is enabled by default.

  - The ASA can simultaneously support standard IPsec, IPsec over TCP, NAT-T, and IPsec over UDP, depending on the client with which it is exchanging data.
  - When both NAT-T and IPsec over UDP are enabled, NAT-T takes precedence.
  - When enabled, IPsec over TCP takes precedence over all other connection methods.

  The ASA implementation of NAT-T supports IPsec peers behind a single NAT/PAT device as follows:

  - One LAN-to-LAN connection.
  - Either a LAN-to-LAN connection or multiple remote access clients, but not a mixture of both.

  To use NAT-T you must:

  - Create an ACL for the interface you will be using to open port 4500 (Configuration > Firewall > Access Rules).
  - Enable IPsec over NAT-T in this pane.
  - On the Fragmentation Policy parameter in the Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies pane, edit the interface you will be using to Enable IPsec pre-fragmentation. When this is configured, it is still alright to let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do.

- Enable IPsec over TCP

  IPsec over TCP enables a VPN client to operate in an environment in which standard ESP or IKE cannot function, or can function only with modification to existing firewall rules. IPsec over TCP encapsulates both the IKE and IPsec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature is disabled by default.

Note This feature does not work with proxy-based firewalls.

IPsec over TCP works with remote access clients. It works on all physical and VLAN interfaces. It is a client to ASA feature only. It does not work for LAN-to-LAN connections.

- The ASA can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the ASA and the client to which it connects.

You can enable IPsec over TCP for up to 10 ports that you specify. If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work. The consequence is that you can no longer use a browser to manage the ASA through the IKE-enabled interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the ASA. The client configuration must include at least one of the ports you set for the ASA.

Identity Sent to Peer

Choose the **Identity** that the peers will use to identify themselves during IKE negotiations:

Address	Uses the IP addresses of the hosts exchanging ISAKMP identity information.
Hostname	Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
Key ID	Uses the remote peer uses the **Key Id String** that you specify to look up the preshared key.
Automatic	Determines IKE negotiation by connection type: • IP address for preshared key • Cert DN for certificate authentication.

Session Control

- Disable Inbound Aggressive Mode Connections

  Phase 1 IKE negotiations can use either Main mode or Aggressive mode. Both provide the same services, but Aggressive mode requires only two exchanges between the peers, rather than three. Aggressive mode is faster, but does not provide identity protection for the communicating parties. It is therefore necessary that they exchange identification information prior to establishing a secure SA in which to encrypt in formation. This feature is disabled by default.

- Alert Peers Before Disconnecting
  - Client or LAN-to-LAN sessions may be dropped for several reasons, such as: a ASA shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.
  - The ASA can notify qualified peers (in LAN-to-LAN configurations) of sessions that are about to be disconnected, and it conveys to them the reason. The peer or client receiving the alert decodes the reason and displays it in the event log or in a pop-up pane. This feature is disabled by default.
  - This pane lets you enable the feature so that the ASA sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- Security appliances with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).

- Wait for All Active Sessions to Voluntarily Terminate Before Rebooting

  You can schedule a ASA reboot to occur only when all active sessions have terminated voluntarily. This feature is disabled by default.

- Number of SAs Allowed in Negotiation for IKEv1

  Limits the maximum number of SAs that can be in negotiation at any time.

IKE v2 Specific Settings

Additional session controls are available for IKE v2, that limit the number of open SAs. By default, the ASA does not limit the number of open SAs:

- Cookie Challenge—Enables the ASA to send cookie challenges to peer devices in response to SA initiate packets.
  - % threshold before incoming SAs are cookie challenged—The percentage of the total allowed SAs for the ASA that are in-negotiation, which triggers cookie challenges for any future SA negotiations. The range is zero to 100%. The default is 50%.
- Number of Allowed SAs in Negotiation—Limits the maximum number of SAs that can be in negotiation at any time. If used in conjunction with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check.
- Maximum Number of SAs Allowed—Limits the number of allowed IKEv2 connections on the ASA. By default, the limit is the maximum number of connections specified by the license.
- Maximum Number of Queues Allowed—Limits the number of allowed queues on the ASA.
- Notify Invalid Selector—Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. Sending this notification is disabled by default.
- Enable Fragmentation—Enables fragmentation for an IKEv2 VPN on an ASA.
- Fragmentation MTU—Specify a maximum transmission unit (MTU) size between 200 and 1500 bytes.
- Preferred Fragmentation Method:
  - IETF RFC-7383—Select this method when both peers specify support and preference during negotiation. Using this method, encryption is done after fragmentation providing individual protection for each IKEv2 fragment message.
  - Cisco proprietary method—Select this method when it is the only method provided by a peer, such as the AnyConnect Client, or if both peers specify support and preference during negotiation. Using this method fragmentation is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received. This method does not interoperate with non-Cisco peers.

Preventing DoS Attacks with IKE v2 Specific Settings

You can prevent denial-of-service (DoS) attacks for IPsec IKEv2 connections by configuring Cookie Challenge, which challenges the identify of incoming Security Associations (SAs), or by limiting the number of open SAs. By default, the ASA does not limit the number of open SAs, and never cookie challenges SAs. You can also limit the number of SAs allowed, which stops further connections from negotiating to protect against memory and/or CPU attacks that the cookie-challenge feature may be unable to thwart and protects the current connections.

With a DoS attack, an attacker initiates the attack when the peer device sends an SA initiate packet and the ASA sends its response, but the peer device does not respond further. If the peer device does this continually, all the allowed SA requests on the ASA can be used up until it stops responding.

Enabling a threshold percentage for cookie challenging limits the number of open SA negotiations. For example, with the default setting of 50%, when 50% of the allowed SAs are in-negotiation (open), the ASA cookie challenges any additional SA initiate packets that arrive.

If used in conjunction with the **Number of SAs Allowed in Negotiation**, or the Maximum Number of SAs Allowed, configure the cookie-challenge threshold lower than these settings for an effective cross-check.

You can also limit the life on all SAs at the IPsec level by choosing Configuration > Site-to-Site VPN > Advanced > System Options.

About IKEv2 Multi-Peer Crypto Map

Beginning with the 9.14(1) release, ASA IKEv2 supports multi-peer crypto map—when a peer in a tunnel goes down, IKEv2 attempts to establish the tunnel with the next peer in the list. You can configure crypto map with a maximum of 10 peer addresses. This multiple peer support on IKEv2 is useful, especially, when you are migrating from IKEv1 with multi-peer crypto maps.

IKEv2 supports only bi-directional crypto maps. Hence, the multiple peers are also configured on bi-directional crypto maps, and the same is used to accept the request from peers initiating the tunnel.

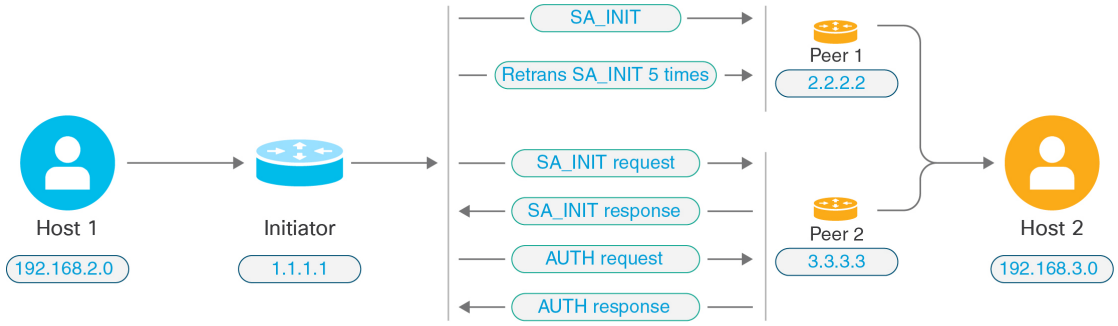
IKEv2 Initiator Behavior

IKEv2 initiates session with a peer, say Peer1. If Peer1 is unreachable for 5 SA_INIT retransmits, a final retransmit is sent. This activity takes about 2 minutes.

When Peer1 fails, the SA_INIT message is sent to Peer2. If Peer2 is also unreachable, session establishment is initiated with Peer3 after 2 minutes.

After all the peers are exhausted in the peer list of the crypto map, IKEv2 initiates the session again from Peer1 until a SA is established with any of the peers. The following figure depicts this behavior.

Figure 1: Initiator Process Flow



Note Continuous traffic is required to initiate IKE SA so that each failure attempt would move to the next peer and finally some reachable peer establishes the SA. In cases of disrupted traffic, a manual trigger is needed to initiate the IKE SA with the next peer.

IKEv2 Responder Behavior

If the responder device of IKE SA is configured with multiple peers in the crypto map, whenever an IKE SA is attempted, the address of the initiator IKE SA is validated with that of the current active peer in the crypto map.

For example, if the current active peer in the crypto map (being used as Responder) is the first peer, then the IKE SA is initiated from Peer1 IP address. Similarly, if the current active peer in the crypto map (being used as Responder) is the second peer, then IKE SA is initiated from Peer2 IP address.

Note Peer traversal is not supported on the Responder Side of a IKEv2 multi-peer topology.

Peer Index Reset Upon Crypto Map Changes

Any change to the crypto map resets the peer index to zero, and the tunnel initiation starts from first peer in the list. Following table provides multiple peer index transition under specific conditions:

Table 1: Multi-Peer Index Transition before SA

Conditions prior to SA	Peer Index Moved Yes/No/Reset
Peer not reachable	Yes
Phase 1 proposal mismatch	Yes
Phase 2 proposal mismatch	Yes

Conditions prior to SA	Peer Index Moved Yes/No/Reset
DPD ack not received	Yes
Traffic selectors mismatch during AUTH phase	Yes
Authentication failure	Yes
Rekey failure due to peer not reachable	Reset

Table 2: Multi-Peer Index Transition after SA

Conditions after SA	Peer Index Moved Yes/No/Reset
Rekey failure due to proposal mismatch	Reset
Traffic selectors mismatch during rekey	Reset
Crypto map modification	Reset
HA switchover	No
Clear crypto IKEv2 SA	Reset
Clear ipsec sa	Reset
IKEv2 SA timeout	Reset

Guidelines for IKEv2 Multi-Peer

IKEv1 and IKEv2 Protocols

If a crypto map is configured with both the IKE versions and multiple peers, SA attempt is made on each peer with both versions before moving to next peer.

For example, if a crypto map is configured with two peers, say P1 and P2, then the tunnel is initiated to P1 with IKEv2, P1 with IKEv1, P2 with IKEv2, and so on.

High Availability

A crypto map with multiple peers initiates tunnels to the Responder device that is in HA. It moves to the next Responder device when the first device isn't reachable.

An initiator device initiates tunnels to the Responder device. If the active device goes down, the standby device attempts to establish the tunnel from the Peer1 IP address, irrespective of the crypto map moving to the Peer2 IP address on the active device.

Centralized Cluster

A crypto map with multiple peers can initiate tunnels to the Responder device that is in a Centralized cluster deployment. If the first device is unreachable, it attempts to move to the next Responder device.

An initiator device initiates tunnels to the Responder device. Every node in the cluster moves to the next Peer2, if Peer1 isn't reachable.

Distributed Cluster

Distributed clustering isn't supported when an IKEv2 multi-peer crypto map is configured.

Multiple Context Modes

In multiple context modes, multi-peer behavior is specific to each context.

Debug Command

If the tunnel establishment fails, enable these commands to further analyse the issue.

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

The following example is that of a debug log that is specific to IKEv2 multi-peer, which displays the transition of peers.

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto map.
```

IKE Policies

Configuration > Site-to-Site VPN > Advanced > IKE Policies

Use this pane to Add, Edit, or Delete IKEv1 and IKEv2 Policies.

To set the terms of the IKE negotiations, you create one or more IKE policies, which include the following:

- A unique priority (1 through 65,543, with 1 the highest priority).
- An authentication method, to ensure the identity of the peers.
- An encryption method, to protect the data and ensure privacy.
- An HMAC method to ensure the identity of the sender, and to ensure that the message has not been modified in transit.
- A Diffie-Hellman group to establish the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.
- A limit for how long the ASA uses an encryption key before replacing it.

Each IKE negotiation is divided into two sections called Phase1 and Phase 2. Phase 1 creates the first tunnel, which protects later IKE negotiation messages. Phase 2 creates the tunnel that protects data.

For IKEv1, you can only enable one setting for each parameter. For IKEv2, each proposal can have multiples settings for Encryption, D-H Group, Integrity Hash, and PRF Hash.

If you do not configure any IKE policies, the ASA uses the default policy, which is always set to the lowest priority, and which contains the default value for each parameter. If you do not specify a value for a specific parameter, the default value takes effect.

When IKE negotiation begins, the peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order.

A match between IKE policies exists if they have the same encryption, hash, authentication, and Diffie-Hellman values, and an SA lifetime less than or equal to the lifetime in the policy sent. If the lifetimes are not identical, the shorter lifetime—from the remote peer policy—applies. If no match exists, IKE refuses negotiation and the IKE SA is not established.

Fields

- IKEv1 Policies—Displays parameter settings for each configured IKE policy.
  - Priority #—Shows the priority of the policy.
  - Encryption—Shows the encryption method.
  - Hash—Shows the hash algorithm.
  - D-H Group—Shows the Diffie-Hellman group.
  - Authentication—Shows the authentication method.
  - Lifetime (secs)—Shows the SA lifetime in seconds.
- IKEv2 Policies—Displays parameter settings for each configured IKEv2 policy.
  - Priority #—Shows the priority of the policy.
  - Encryption—Shows the encryption method.
  - Integrity Hash—Shows the hash algorithm.
  - PRF Hash—Shows the pseudo random function (PRF) hash algorithm.
  - D-H Group—Shows the Diffie-Hellman group.
  - Lifetime (secs)—Shows the SA lifetime in seconds.

Add or Edit an IKEv1 Policy

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKE Policy

Priority #—Type a number to set a priority for the IKE policy. The range is 1 to 65535, with 1 the highest priority.

Encryption—Choose an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers.The choices follow:

des	56-bit DES-CBC. Less secure but faster than the alternatives. The default.
3des	168-bit Triple DES.
aes	128-bit AES.
aes-192	192-bit AES.
aes-256	256-bit AES.

Hash—Choose the hash algorithm that ensures data integrity. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	

Authentication—Choose the authentication method the ASA uses to establish the identity of each IPsec peer. Preshared keys do not scale well with a growing network, but are easier to set up in a small network. The choices follow:

pre-share	Preshared keys.
rsa-sig	A digital certificate with keys generated by the RSA signatures algorithm.

D-H Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 1or 5.
2	Group 2 (1024-bit)	
5	Group 5 (1536-bit)	
14	Group 14 (2048-bit)	The default Diffie-Hellman group is, Group 14 (2048-bit Diffie-Hellman)

Lifetime (secs)—Either check Unlimited or enter an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the ASA sets up future IPsec security associations less quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Time Measure—Choose a time measure. The ASA accepts the following values:.

120 - 86,400 seconds
2 - 1440 minutes
1 - 24 hours
1 day

Add or Edit an IKEv2 Policy

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy

Priority #—Type a number to set a priority for the IKEv2 policy. The range is 1 to 65535, with 1 the highest priority.

Encryption—Choose an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers.The choices follow:

des	Specifies 56-bit DES-CBC encryption for ESP.

3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies AES-GCM/GMAC 128-bit support for symmetric encryption and integrity.
aes-gcm-192	Specifies AES-GCM/GMAC 192-bit support for symmetric encryption and integrity.
aes-gcm-256	Specifies AES-GCM/GMAC 256-bit support for symmetric encryption and integrity.
NULL	Indicates no encryption.

D-H Group—Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	The default, Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 or 5.
2	Group 2 (1024-bit)	
5	Group 5 (1536-bit)	
14	Group 14	
19	Group 19	
20	Group 20	
21	Group 21	
24	Group 24	

Integrity Hash—Choose the hash algorithm that ensures data integrity for the ESP protocol. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA 1	The default is SHA 1. MD5 has a smaller digest and is considered to be slightly faster than SHA 1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	
sha256	SHA 2, 256-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	**SHA 2, 384-bit digest**	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	**SHA 2, 512-bit digest**	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

null		Indicates that AES-GCM or AES-GMAC is configured as the encryption algorithm. You must choose the null integrity algorithm if AES-GCM has been configured as the encryption algorithm.

Pseudo-Random Function (PRF)—Specify the PRF used for the construction of keying material for all of the cryptographic algorithms used in the SA..

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	
sha256	SHA 2, 256-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	SHA 2, 384-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	SHA 2, 512-bit digest	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Lifetime (secs)—Either check Unlimited or enter an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the ASA sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

The ASA accepts the following values:.

120 - 86,400 seconds
2 - 1440 minutes
1 - 24 hours
1 day

Configure IPsec

The ASA uses IPsec for LAN-to-LAN VPN connections, and provides the option of using IPsec for client-to-LAN VPN connections. In IPsec terminology, a “peer” is a remote-access client or another secure gateway.The ASA supports LAN-to-LAN IPsec connections with Cisco peers (IPv4 or IPv6), and with third-party peers that comply with all relevant standards.

During tunnel establishment, the two peers negotiate security associations that govern authentication, encryption, encapsulation, and key management. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPsec SA).

A LAN-to-LAN VPN connects networks in different geographic locations. In IPsec LAN-to-LAN connections, the ASA can function as initiator or responder. In IPsec client-to-LAN connections, the ASA functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The ASA supports these IPsec attributes:

- Main mode for negotiating phase one ISAKMP security associations when using digital certificates for authentication
- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Encryption Algorithms:
  - AES-128, -192, and -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

Procedure

Step 1 Configure Crypto Maps, on page 25.
Step 2 Configure IPsec Pre-Fragmentation Policies, on page 33.
Step 3 Configure IPsec Proposals (Transform Sets), on page 35.

Crypto Maps

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

This pane shows the currently configured crypto maps, which are defined in IPsec rules. Here you can add, edit, delete and move up, move down, cut, copy, and paste an IPsec rule.

Note You cannot edit, delete, or copy an implicit rule. The ASA implicitly accepts the traffic selection proposal from remote clients when configured with a dynamic tunnel policy. You can override it by giving a specific traffic selection.

You can also **Find** (filter the display of) rules by selecting Interface, Source, Destination, Destination Service, or Rule Query, selecting is or contains, and entering the filter parameter. Click ... to launch a browse dialog box that displays all existing entries that you can choose. Use **Diagram** to display the rules pictorially.

The IPsec rules specify the following:

- Type: Priority—Displays the type of rule (static or dynamic) and its priority.
- Traffic Selection
  - #—Indicates the rule number.
  - Source—Indicates the IP addresses that are subject to this rule when traffic is sent to the IP addresses listed in the Remote Side Host/Network column. In detail mode (see the Show Detail button), an address column might contain an interface name with the word any, such as inside:any. any means that any host on the inside interface is affected by the rule.
  - Destination—Lists the IP addresses that are subject to this rule when traffic is sent from the IP addresses listed in the Security Appliance Side Host/Network column. In detail mode (see the Show Detail button), an address column might contain an interface name with the word any, such as outside:any. any means that any host on the outside interface is affected by the rule. Also in detail mode, an address column might contain IP addresses in square brackets, for example, [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the ASA maps the inside host's address to an address from the pool. After a host creates an outbound connection, the ASA maintains this address mapping. This address mapping structure is called an xlate, and remains in memory for a period of time.
  - Service—Specifies the service and protocol specified by the rule (TCP, UDP, ICMP, or IP).
  - Action—Specifies the type of IPsec rule (protect or do not protect).
- Transform Set—Displays the transform set for the rule.
- Peer—Identifies the IPsec peer.
- PFS—Displays perfect forward secrecy settings for the rule.
- NAT-T Enabled—Indicates whether NAT Traversal is enabled for the policy.
- Reverse Route Enabled—Indicates whether Reverse Route Injection (RRI) is enabled for the policy. RRI is done upon configuration and is considered static, remaining in place until the configuration changes or is removed. The ASA automatically adds static routes to the routing table and announces these routes to its private network or border routers using OSPF.
  - Dynamic— If dynamic is specified, RRIs are created upon the successful establishment of IPsec security associations (SA's) and deleted after the IPsec SA's are deleted.

Note Dynamic RRI applies to IKEv2 based static crypto maps only.

- Connection Type—(Meaningful only for static tunnel policies.) Identifies the connection type for this policy as bidirectional, originate-only, or answer-only).
- SA Lifetime—Displays the SA lifetime for the rule.
- CA Certificate—Displays the CA certificate for the policy. This applies to static connections only.
- IKE Negotiation Mode—Displays whether IKE negotiations use main or aggressive mode.
- Description—(Optional) Specifies a brief description for this rule. For an existing rule, this is the description you typed when you added the rule. An implicit rule includes the following description: "Implicit rule." To edit the description of any but an implicit rule, right-click this column, and choose Edit Description or double-click the column.
- Enable Anti-replay window size—Sets the anti-replay window size, between 64 and 1028 in multiples of 64. One side-effect of priority queueing in a hierarchical QoS policy with traffic shaping (see "Rule Actions > QoS Tab") is packet re-ordering. For IPsec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings becomes false alarms in the case of priority queueing. Configuring the anti-replay pane size helps you avoid possible false alarms.
- Enable IPsec Inner Routing Lookup—By default lookups are not done for packets sent through the IPsec tunnel, per-packet adjacency lookups are done only for the outer ESP packets, In some network topologies, when a routing update has altered the inner packet's path, but the local IPsec tunnel is still up, packets through the tunnel may not be routed correctly and fail to reach their destination. To prevent this, enable per-packet routing lookups for the IPsec inner packets.

Create or Edit an IPsec Rule Tunnel Policy (Crypto Map) - Basic Tab

Use this pane to define a new Tunnel Policy for an IPsec rule. The values you define here appear in the IPsec Rules table after you click **OK**. All rules are enabled by default as soon as they appear in the IPsec Rules table.

The Tunnel Policy pane lets you define a tunnel policy that is used to negotiate an IPsec (Phase 2) security association (SA). ASDM captures your configuration edits, but does not save them to the running configuration until you click **Apply**.

Every tunnel policy must specify a transform set and identify the security appliance interface to which it applies. The transform set identifies the encryption and hash algorithms that perform IPsec encryption and decryption operations. Because not every IPsec peer supports the same algorithms, you might want to specify a number of policies and assign a priority to each. The security appliance then negotiates with the remote IPsec peer to agree on a transform set that both peers support.

Tunnel policies can be *static* or *dynamic*. A static tunnel policy identifies one or more remote IPsec peers or subnetworks to which your security appliance permits IPsec connections. A static policy can be used whether your security appliance initiates the connection or receives a connection request from a remote host. A static policy requires you to enter the information necessary to identify permitted hosts or networks.

A dynamic tunnel policy is used when you cannot or do not want to provide information about remote hosts that are permitted to initiate a connection with the security appliance. If you are only using your security appliance as a VPN client in relation to a remote VPN central-site device, you do not need to configure any

dynamic tunnel policies. Dynamic tunnel policies are most useful for allowing remote access clients to initiate a connection to your network through a security appliance acting as the VPN central-site device. A dynamic tunnel policy is useful when the remote access clients have dynamically assigned IP addresses or when you do not want to configure separate policies for a large number of remote access clients.

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Basic

- Interface—Choose the interface name to which this policy applies.
- Policy Type—Choose the type, static or dynamic, of this tunnel policy.
- Priority—Enter the priority of the policy.
- IKE Proposals (Transform Sets)--Specifies IKEv1 and IKEv2 IPsec proposals:
  - IKEv1 IPsec Proposal—Choose the proposal (transform set) for the policy and click **Add** to move it to the list of active transform sets. Click **Move Up** or **Move Down** to rearrange the order of the proposals in the list box. You can add a maximum of 11 proposals to a crypto map entry or a dynamic crypto map entry.
  - IKEv2 IPsec Proposal—Choose the proposal (transform set) for the policy and click **Add** to move it to the list of active transform sets. Click **Move Up** or **Move Down** to rearrange the order of the proposals in the list box. You can add a maximum of 11 proposals to a crypto map entry or a dynamic crypto map entry.
- Peer Settings - Optional for Dynamic Crypto Map Entries—Configure the peer settings for the policy.
  - Connection Type—(Meaningful only for static tunnel policies.) Choose bidirectional, originate-only, or answer-only to specify the connection type of this policy. For LAN-to-LAN connections, choose bidirectional or answer-only (not originate-only). Choose answer-only for LAN-to-LAN redundancy. If you choose Originate Only, you can specify up to 10 redundant peers. For uni-directional, you can specify originate only or answer only, and neither are enabled by default.
  - IP Address of Peer to Be Added—Enter the IP address of the IPsec peer you are adding. Beginning with 9.14(1), ASA supports multiple peers in IKEv2. You can add a maximum of 10 peers to the crypto map.
- Enable Perfect Forwarding Secrecy—Check to enable perfect forward secrecy for the policy. PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless you specify Perfect Forward Secrecy.
- Diffie-Hellman Group—When you enable PFS you must also choose a Diffie-Hellman group which the ASA uses to generate session keys. The choices are as follows:
  - Group 1 (768-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 1 to generate IPsec session keys, where the prime and generator numbers are 768 bits. This option is more secure but requires more processing overhead.
  - Group 2 (1024-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 2 to generate IPsec session keys, where the prime and generator numbers are 1024 bits. This option is more secure than Group 1 but requires more processing overhead.
  - Group 5 (1536-bits) = Use perfect forward secrecy, and use Diffie-Hellman Group 5 to generate IPsec session keys, where the prime and generator numbers are 1536 bits. This option is more secure than Group 2 but requires more processing overhead.

- Group 14 (2048-bits) = Use perfect forward secrecy and use Diffie-Hellman Group 14 for IKEv2.
- Group 19= Use perfect forward secrecy and use Diffie-Hellman Group 19 for IKEv2 to support ECDH.
- Group 20= Use perfect forward secrecy and use Diffie-Hellman Group 20 for IKEv2 to support ECDH.
- Group 21= Use perfect forward secrecy and use Diffie-Hellman Group 21 for IKEv2 to support ECDH.
- Group 24= Use perfect forward secrecy and use Diffie-Hellman Group 24 for IKEv2.

Create or Edit IPsec Rule Tunnel Policy (Crypto Map) - Advanced Tab

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced

- Enable NAT-T— Enables NAT Traversal (NAT-T) for this policy.
- Enable Reverse Route Injection—Enables Reverse Route Injection for this policy. Reverse Route Injection (RRI) is used to populate the routing table of an internal router that runs dynamic routing protocols such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) if you run ASA, or Routing Information Protocol (RIP) for remote VPN Clients or LAN to LAN sessions. RRI is done upon configuration and is considered static, remaining in place until the configuration changes or is removed. The ASA automatically adds static routes to the routing table and announces these routes to its private network or border routers using OSPF. Do not enable RRI if you specify any source/destination (0.0.0.0/0.0.0.0) as the protected network, because this will impact traffic that uses your default route.
  - Dynamic— If dynamic is specified, RRIs are created upon the successful establishment of IPsec security associations (SA's) and deleted after the IPsec SA's are deleted. Typically, RRI routes are used to Initiate a tunnel if one is not present and traffic needs to be encrypted. With dynamic RRI support, no routes are present before the tunnel is brought up. Therefore, an ASA with dynamic RRI configured would typically work only as a responder.



Note Dynamic RRI applies to IKEv2 based static crypto maps only.

- Security Association Lifetime Settings—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
  - Time—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
  - Traffic Volume—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Static Type Only Settings—Specifies parameters for static tunnel policies.
  - Device Certificate—Choose the certificate to use. If you choose something other than None (Use Preshared Keys), which is the default. The Send CA certificate chain check box becomes active when you choose something other than None.

- Send CA certificate chain—Enables transmission of the entire trust point chain.
- IKE Negotiation Mode—Chooses the IKE negotiation mode, Main or Aggressive. This parameter sets the mode for exchanging key information and setting up the SAs. It sets the mode that the initiator of the negotiation uses; the responder auto-negotiates. Aggressive Mode is faster, using fewer packets and fewer exchanges, but it does not protect the identity of the communicating parties. Main Mode is slower, using more packets and more exchanges, but it protects the identities of the communicating parties. This mode is more secure and it is the default selection. If you choose Aggressive, the Diffie-Hellman Group list becomes active.
- Diffie-Hellman Group—Choose the Diffie-Hellman group to apply. The choices are as follows: Group 1 (768-bits), Group 2 (1024-bits), or Group 5 (1536-bits).

- ESP v3—Specify whether incoming ICMP error messages are validated for cryptography and dynamic cryptography maps, set the per-security association policy, or enable traffic flow packets:
  - Validate incoming ICMP error messages—Choose whether to validate those ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.
  - Enable Do Not Fragment (DF) policy—Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header. Choose one of the following:

    Clear DF bit—Ignores the DF bit.

    Copy DF bit—Maintains the DF bit.

    Set DF bit—Sets and uses the DF bit.
  - Enable Traffic Flow Confidentiality (TFC) packets—Enable dummy TFC packets that mask the traffic profile which traverses the tunnel.



Note You must have an IKE v2 IPsec proposal set on the Tunnel Policy (Crypto Map) Basic tab before enabling TFC.

Use the Burst, Payload Size, and Timeout parameters to generate random length packets at random intervals across the specified SA.

Create or Edit IPsec Rule Traffic Selection Tab

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Traffic Selection

This pane lets you define what traffic to protect (permit) or not protect (deny).

- Action—Specify the action for this rule to take. The selections are protect and do not protect.
- Source—Specify the IP address, network object group or interface IP address for the source host or network. A rule cannot use the same address as both the source and destination. Click ... to launch the Browse Source dialog box that contains the following fields:
  - Add/Edit—Choose IP Address or Network Object Group to add more source addresses or groups.
  - Delete—Click to delete an entry.

- Filter—Enter an IP Address to filter the results displayed.
- Name—Indicates that the parameters that follow specify the name of the source host or network.
- IP Address—Indicates that the parameters that follow specify the interface, IP address, and subnet mask of the source host or network.
- Netmask—Chooses a standard subnet mask to apply to the IP address. This parameter appears when you choose the IP Address option button.
- Description—Enter a description.
- Selected Source—Click **Source** to include the selected entry as a source.

- Destination—Specify the IP address, network object group or interface IP address for the destination host or network. A rule cannot use the same address as both the source and destination. Click ... to launch the Browse Destination dialog box that contains the following fields:
  - Add/Edit—Choose IP Address or Network Object Group to add more destination addresses or groups.
  - Delete—Click to delete an entry.
  - Filter—Enter an IP Address to filter the results displayed.
  - Name—Indicates that the parameters that follow specify the name of the destination host or network.
  - IP Address—Indicates that the parameters that follow specify the interface, IP address, and subnet mask of the destination host or network.
  - Netmask—Chooses a standard subnet mask to apply to the IP address. This parameter appears when you choose the IP Address option button.
  - Description—Enter a description.
  - Selected Destination—Click **Destination** to include the selected entry as a destination.

- Service—Enter a service or click ... to launch the browse service dialog box where you can choose from a list of services.
- Description—Enter a description for the Traffic Selection entry.
- More Options
  - Enable Rule—Click to enable this rule.
  - Source Service—Enter a service or click **...** to launch the browse service dialog box where you can choose from a list of services.
  - Time Range—Define a time range for which this rule applies.
  - Group—Indicates that the parameters that follow specify the interface and group name of the source host or network.
  - Interface—Choose the interface name for the IP address. This parameter appears when you choose the IP Address option button.
  - IP address—Specifies the IP address of the interface to which this policy applies. This parameter appears when you choose the IP Address option button.

- Destination—Specify the IP address, network object group or interface IP address for the source or destination host or network. A rule cannot use the same address as both the source and destination. Click **...** for either of these fields to launch the Browse dialog box that contains the following fields:
- Name—Choose the interface name to use as the source or destination host or network. This parameter appears when you choose the Name option button. This is the only parameter associated with this option.
- Interface—Choose the interface name for the IP address. This parameter appears when you click the Group option button.
- Group—Choose the name of the group on the specified interface for the source or destination host or network. If the list contains no entries, you can enter the name of an existing group. This parameter appears when you click the Group option button.

- **Protocol and Service**—Specifies protocol and service parameters relevant to this rule.



Note "Any - any" IPsec rules are not allowed. This type of rule would prevent the device and its peer from supporting multiple LAN -to-LAN tunnels.

- TCP—Specifies that this rule applies to TCP connections. This selection also displays the Source Port and Destination Port group boxes.
- UDP—Specifies that this rule applies to UDP connections. This selection also displays the Source Port and Destination Port group boxes.
- ICMP—Specifies that this rule applies to ICMP connections. This selection also displays the ICMP Type group box.
- IP—Specifies that this rule applies to IP connections. This selection also displays the IP Protocol group box.
- Manage Service Groups—Displays the Manage Service Groups pane, on which you can add, edit, or delete a group of TCP/UDP services/ports.
- Source Port and Destination Port —Contains TCP or UDP port parameters, depending on which option button you chose in the Protocol and Service group box.
- Service—Indicates that you are specifying parameters for an individual service. Specifies the name of the service and a boolean operator to use when applying the filter.
- Boolean operator (unlabeled)—Lists the boolean conditions (equal, not equal, greater than, less than, or range) to use in matching the service specified in the service box.
- Service (unlabeled)—Identifies the service (such as https, ldaps, or any) to be matched. If you specified the range service operator this parameter becomes two boxes, into which you enter the start and the end of the range.
- ... —Displays a list of services from which you can choose the service to display in the Service box.
- Service Group—Indicates that you are specifying the name of a service group for the source port.
- Service (unlabeled)—Choose the service group to use.

- ICMP Type—Specifies the ICMP type to use. The default is any. Click the **...** button to display a list of available types.

- Options
  - Time Range—Specify the name of an existing time range or create a new range.
  - ... —Displays the Add Time Range pane, on which you can define a new time range.
  - Please enter the description below (optional)—Provides space for you to enter a brief description of the rule.

IPsec Pre-Fragmentation Policies

Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies

The IPsec pre-fragmentation policy specifies how to treat packets that exceed the maximum transmission unit (MTU) setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the ASA and the client rejects or drops IP fragments. For example, suppose a client wants to FTP get from an FTP server behind a ASA. The FTP server transmits packets that when encapsulated would exceed the ASA's MTU size on the public interface. The selected options determine how the ASA processes these packets. The pre-fragmentation policy applies to all traffic travelling out the ASA public interface.

The ASA encapsulates all tunneled packets. After encapsulation, the ASA fragments packets that exceed the MTU setting before transmitting them through the public interface. This is the default policy. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices may drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.

When you enable pre-fragmentation, the ASA fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the ASA clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site. In our example, the ASA overrides the MTU and allows fragmentation by clearing the DF bit.

Note Changing the MTU or the pre-fragmentation option on any interface tears down all existing connections. For example, if 100 active tunnels terminate on the public interface, and you change the MTU or the pre-fragmentation option on the external interface, all of the active tunnels on the public interface are dropped.

Use this pane to view or **Edit** an existing IPsec pre-fragmentation policy and do-not-fragment (DF) bit policy for an interface selected on the parent pane.

Fields

- **Interface**—Identifies the chosen interface. You cannot change this parameter using this dialog box.
- **Pre-fragmentation Enabled**—Enables or disables IPsec pre-fragmentation. The ASA fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the ASA clears the DF bit, fragments the packets, and then encapsulates them. This action creates two

independent, non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site.

- **DF Bit Setting Policy**—The do-not-fragment bit policy: Copy, Clear, or Set.

Configure IKEv2 Fragmentation Options

On the ASA, IKEv2 fragmentation can be enabled or disabled, the MTU (Maximum Transmission Unit) used when fragmenting IKEv2 packets can be specified, and a preferred fragmentation method can be configured by the administrator on the following screen:

Configuration > **Site-to-Site VPN** > **Advanced** > **IKE parameters**

By default, all methods of IKEv2 fragmentation are enabled, the MTU is 576 for IPv4, or 1280 for IPv6, and the preferred method is the IETF standard RFC-7383.

Specify the MTU with the following considerations:

- The MTU value used should include the IP(IPv4/IPv6) header + UDP header size.
- If not specified by the administrator the default MTU is 576 for IPv4, or 1280 for IPv6.
- Once specified, the same MTU will be used for both IPv4 and IPv6.
- Valid range is 68-1500.



Note You must consider the ESP overhead while configuring the MTU. The packet size increases after encryption due to the ESP overhead that is added to the MTU during the encryption. If you get the "packet too big" error, ensure that you check the MTU size and configure a lower MTU.

One of the following supported fragmentation methods can be configured as the preferred fragmentation method for IKEv2:

- IETF RFC-7383 standard based IKEv2 fragmentation.
  - This method will be used when both peers specify support and preference during negotiation.
  - Using this method, encryption is done after fragmentation providing individual protection for each IKEv2 Fragment message.
- Cisco proprietary fragmentation.
  - This method will be used if it is the only method provided by a peer, such as the AnyConnect Client, or if both peers specify support and preference during negotiation.
  - Using this method fragmentation is done after encryption. The receiving peer cannot decrypt or authenticate the message until all fragments are received.
  - This method does not interoperate with non-Cisco peers.

Before you begin

- Path MTU Discovery is not supported, the MTU needs to be manually configured to match the needs of the network.
- This configuration is global and will affect future SAs established after the configuration has been applied. Older SAs will not be affected. Same behavior holds true when fragmentation is disabled.
- A maximum of a 100 fragments can be received.

Procedure

Step 1 In ASDM go to **Configuration** > **Site-to-Site VPN** > **Advanced** > **IKE parameters**.

Step 2 Select or deselect the **Enable fragmentation** field.

Step 3 Specify the **Fragmentation MTU** size.

Step 4 Specify the **Preferred fragmentation method**.

IPsec Proposals (Transform Sets)

Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets)

A transform is a set of operations done on a data flow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with 3DES encryption and the HMAC-MD5 authentication algorithm (ESP-3DES-MD5).

Use this pane to view, **Add**, **Edit**, or **Delete** IKEv1 and IKEv2 transform sets described below. Each table displays the name and details of the configured transform sets.

IKEv1 IPsec Proposals (Transform Sets)

- **Mode**—Mode for applying ESP encryption and authentication. This determines what part of the original IP packet has ESP applied.
  - **Tunnel mode**—(default) Applies ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses.The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPsec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.
  - **Transport mode**—Only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.

- **ESP Encryption**—Encapsulating Security Protocol (ESP) encryption algorithms for the transform sets. ESP provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data being protected.
- **ESP Authentication**— ESP authentication algorithms for the transform set.

IKEv2 IPsec Proposals

- **Mode**—Mode for applying ESP encryption and authentication. This determines what part of the original IP packet has ESP applied.
  - **Tunnel mode**—(default) Encapsulation mode will be tunnel mode. Tunnel mode applies ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses.The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet.

    This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system.

    The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPsec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.
  - **Transport mode**— Encapsulation mode will be transport mode with option to fallback on tunnel mode, if peer does not support it. In Transport mode only the IP payload is encrypted, and the original IP headers are left intact.

    This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.
  - **Transport Required**— Encapsulation mode will be transport mode only, falling back to tunnel mode is not allowed.



Note Transport mode is not recommended for Remote Access VPNs.

Examples of negotiation of the encapsulation mode is as follows:

- If the initiator proposes transport mode, and the responder responds with tunnel mode, the initiator will fall back to Tunnel mode.
- If the initiator proposes tunnel mode, and responder responds with transport mode, the responder will fallback to Tunnel mode.
- If the initiator proposes tunnel mode and responder has transport-require mode, then NO PROPOSAL CHOSEN will be sent by the responder.

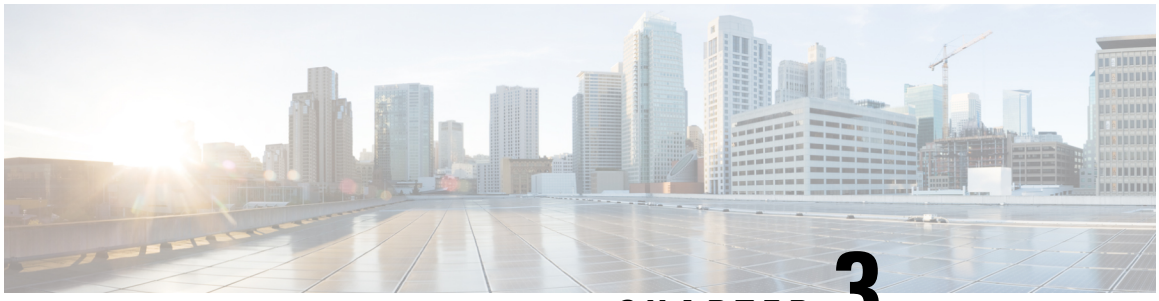
- Similarly if initiator has transport-require, and responder has tunnel mode, NO PROPOSAL CHOSEN will be sent by the responder.

- **Encryption**—Shows the Encapsulating Security Protocol (ESP) encryption algorithms for the IKEv2 IPsec Proposal. ESP provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data being protected.
- **Integrity Hash**—Shows the hash algorithm that ensures data integrity for the ESP protocol. It ensures that a packet comes from whom you would expect and that no modifications were made in transit. It ensures that a packet comes from who you would expect and that no modifications were made in transit. You must choose the null integrity algorithm if AES-GCM/GMAC has been configured as the encryption algorithm.

IPsec Profile

- **Name**—IPsec profile name.
- **IKE v1 IPsec Proposal**—IKE v1 IPsec proposal or the IKE v2 IPsec proposal created for the IPsec profile.
- **Responder only**—Tunnel acts only as a responder.
- **Lifetime**—Security association lifetime duration values in kilobytes and seconds.
- **PFS**—Indicates if PFS is enabled or not.
- **Trustpoint**—Certificate used while initiating the tunnel connection.
- **Local-Identity**—Local IKE identity for the VPN tunnel.
- **Reverse-route**—Indicates if Reverse Route Injection (RRI) is enabled for this IPsec profile.

Security Association (SA) Strength Enforcement—Check this check box to permit connection where the IKEv2 encryption cipher strength is at least equal to the strength of any of its child IPsec SA's encryption ciphers.



CHAPTER 3

High Availability Options

- High Availability Options, on page 39
- VPN Load Balancing, on page 40

High Availability Options

Distributed VPN Clustering, Load balancing and Failover are high-availability features that function differently and have different requirements. In some circumstances you may use multiple capabilities in your deployment. The following sections describe these features. Refer to the appropriate release of the ASA General Operations ASDM Configuration Guide for details on Distributed VPN and Failover. Load Balancing details are included here.

VPN and Clustering on the Secure Firewall eXtensible Operating System (FXOS) Chassis

An ASA FXOS Cluster supports one of two mutually exclusive modes for S2S VPN, centralized or distributed:

- Centralized VPN Mode. The default mode. In centralized mode, VPN connections are established with the control unit of the cluster only.

  VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities. If the control unit fails, all existing VPN connections are lost, and VPN connected users see a disruption in service. When a new control unit is elected, you must reestablish the VPN connections.

  When you connect a VPN tunnel to a Spanned interface address, connections are automatically forwarded to the control unit. VPN-related keys and certificates are replicated to all units.

- Distributed VPN Mode. In this mode, S2S IPsec IKEv2 VPN connections are distributed across members of an ASA cluster providing scalability. Distributing VPN connections across the members of a cluster allows both the capacity and throughput of the cluster to be fully utilized, significantly scaling VPN support beyond Centralized VPN capabilities.

Note Centralized VPN clustering mode supports S2S IKEv1 and S2S IKEv2.

Distributed VPN clustering mode supports S2S IKEv2 only.

Distributed VPN clustering mode is supported on the Firepower 9300 only.

Remote access VPN is not supported in centralized or distributed VPN clustering mode.

VPN Load Balancing

VPN load balancing is a mechanism for equitably distributing remote-access VPN traffic among the devices in a VPN load-balancing group. It is based on simple distribution of traffic without taking into account throughput or other factors. A VPN load-balancing group consists of two or more devices. One device is the director, and the other devices are member devices. Group devices do not need to be of the exact same type, or have identical software versions or configurations.

All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

Failover

A failover configuration requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine when specific failover conditions are met. If those conditions occur, failover occurs. Failover supports both VPN and firewall configurations.

The ASA supports two failover configurations: Active/Active failover and Active/Standby failover.

With Active/Active failover, both units can pass network traffic. This is not true load balancing, although it might appear to have the same effect. When failover occurs, the remaining active unit takes over passing the combined traffic, based on the configured parameters. Therefore, when configuring Active/Active failover, you must make sure that the combined traffic for both units is within the capacity of each unit.

With Active/Standby failover, only one unit passes traffic, while the other unit waits in a standby state and does not pass traffic. Active/Standby failover lets you use a second ASA to take over the functions of a failed unit. When the active unit fails, it changes to the standby state, while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses of the active unit. If an active unit fails, the standby takes over without any interruption to the client VPN tunnel.

VPN Load Balancing

About VPN Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected to the same network to handle remote sessions, you can configure these devices to share their session load by creating a

VPN load-balancing group. VPN Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance an availability.

All devices in the VPN load-balancing group carry session loads. One device in the group, the *director*, directs incoming connection requests to the other devices, called *member devices*. The director monitors all devices in the group, keeps track of how busy each is, and distributes the session load accordingly. The role of director is not tied to a physical device; it can shift among devices. For example, if the current director fails, one of the member devices in the group takes over that role and immediately becomes the new director.

The VPN load-balancing group appears to outside clients as a single, virtual IP address. This IP address is not tied to a specific physical device. It belongs to the current director. A VPN client attempting to establish a connection connects first to the virtual IP address. The director then sends back to the client the public IP address of the least-loaded available host in the group. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the VPN load-balancing group director directs traffic evenly and efficiently across resources.

If an ASA in the group fails, the terminated sessions can immediately reconnect to the virtual IP address. The director then directs these connections to another active device in the group. If the director fails, a member device in the group immediately and automatically takes over as the new director. Even if several devices in the group fail, users can continue to connect to the group as long as any one device in the group is up and available.

For each VPN load balancing cluster device, you must configure the public/outside (lbpublic) and private/inside (lbprivate) interfaces.

- Public interface: The device's outside interface used for initial communication to the cluster IP address. This interface is used for the Hello handshake.
- Private interface: The device's inside interface used for messaging between the load balancing cluster members. These messages include keepalives, topology messages, and out-of-service messages related to load balancing.

VPN Load-Balancing Algorithm

The VPN load-balancing group director maintains a sorted list of group members in ascending IP address order. The load of each member is computed as an integer percentage (the number of active sessions). AnyConnect Client inactive sessions do not count towards the SSL VPN load for VPN load balancing. The director redirects the IPsec and SSL VPN tunnel to the device with the lowest load until it is 1 percent higher than the rest. When all members are 1% higher than the director, the director redirects traffic to itself.

For example, if you have one director and two members, the following cycle applies:



Note All nodes start with 0%, and all percentages are rounded half-up.

1. The director takes the connection if all members have a load at 1% higher than the director.
2. If the director does not take the connection, the session is taken by whichever member device has the lowest load percentage.
3. If all members have the same percentage load, the member with the least number of sessions gets the session.

4. If all members have the same percentage load and the same number of sessions, the member with the lowest IP address gets the session.

VPN Load-Balancing Group Configurations

A VPN load-balancing group can consist of ASAs of the same release or of mixed releases subject to the following restrictions:

- VPN load-balancing groups that consist of both same release ASAs can run VPN load balancing for a mixture of IPsec, AnyConnect Client, and clientless SSL VPN client sessions.
- VPN load-balancing groups that include mixed release ASAs can support IPsec sessions. In such a configuration, however, the ASAs might not reach their full IPsec capacity.

The director of the group assigns session requests to the members of the group. The ASA regards all sessions, SSL VPN or IPsec, as equal, and assigns them accordingly. You can configure the number of IPsec and SSL VPN sessions to allow, up to the maximum allowed by your configuration and license.

We have tested up to 10 nodes in a VPN load-balancing group. Larger groups might work, but we do not officially support such topologies.

VPN Load Balancing Director Election

Director Election Process

Each non-master in the virtual cluster maintains a local topology database. This database is updated by the master whenever the topology of the cluster is changed. Each non-master goes into master election state when either no Hello response is received from the master or no Keepalive response is received from the master after maximum retries.

The member performs the following functions during director election:

- Compares the priority of each load balancing unit found in the local topology database.
- If two units with the same priority are found, one with the lower IP address is elected.
- If the member itself is elected, it claims the virtual IP address.
- If one of the other members is elected, the member sends a Hello request to the elected master.
- When two member units try to claim the virtual IP address, the ARP subsystem detects the duplicate IP address condition and sends a notification to ask the member with higher MAC address to give up the director role.

Hello Handshake

Each member sends a Hello request to the virtual cluster IP address on the outside interface upon startup. If a Hello request is received, the master sends its own Hello request to the member. The non-director member returns a Hello response upon receiving of a Hello request from the director. This concludes the Hello handshake.

Once Hello handshake is completed, the connection is initiated on the inside interface if encryption is configured. If no Hello response is received by the member after maximum retries, the member goes into master election state.

Keepalive Messages

After a Hello handshake is completed between a member and the director, each member unit sends periodic Keepalive requests to the master with its load information. Keepalive requests are sent by a member unit at one second intervals during normal processing if there is no outstanding keepalive responses from the director. This means that the next keepalive request is sent the next second as long as keepalive responses from the previous request was received. If the member did not receive a keepalive response from the director for the previous keepalive request, no keepalive request are sent the next second. Instead, the member's keepalive timeout logic starts.

The keepalive timeout works as follows:

1. If a member is waiting for an outstanding keepalive response from the director, the member does not send the regular one second interval keepalive request.
2. The member waits for 3 seconds and sends a keepalive request at the 4th second.
3. The member repeats step #2 above five(5) times as long as there is no keepalive response from the director.
4. Then, the member declares the director as gone and starts a new director election cycle.

Frequently Asked Questions About VPN Load Balancing

- Multiple Context Mode
- IP Address Pool Exhaustion
- Unique IP Address Pools
- Using VPN Load Balancing and Failover on the Same Device
- VPN Load Balancing on Multiple Interfaces
- Maximum Simultaneous Sessions for VPN Load-Balancing Groups

Multiple Context Mode

Q. Is VPN load balancing supported in multiple context mode?

A. Neither VPN load balancing nor stateful failover is supported in multiple context mode.

IP Address Pool Exhaustion

Q. Does the ASA consider IP address pool exhaustion as part of its VPN load-balancing method?

A. No. If the remote access VPN session is directed to a device that has exhausted its IP address pools, the session does not establish. The load-balancing algorithm is based on load, and is computed as an integer percentage (number of active and maximum sessions) that each member supplies.

Unique IP Address Pools

Q. To implement VPN load balancing, must the IP address pools for AnyConnect Clients or IPsec clients on different ASAs be unique?

A. Yes. IP address pools must be unique for each device.

Using VPN Load Balancing and Failover on the Same Device

Q. Can a single device use both VPN load balancing and failover?

A. Yes. In this configuration, the client connects to the IP address of the group and is redirected to the least-loaded ASA in the group. If that device fails, the standby unit takes over immediately, and there is no impact to the VPN tunnel.

VPN Load Balancing on Multiple Interfaces

Q. If we enable SSL VPN on multiple interfaces, is it possible to implement VPN load balancing for both of the interfaces?

A. You can define only one interface to participate in the VPN load-balancing group as the public interface. The idea is to balance the CPU loads. Multiple interfaces converge on the same CPU, so the concept of VPN load balancing on multiple interfaces does not improve performance.

Maximum Simultaneous Sessions for VPN Load-Balancing Groups

Q. Consider a deployment of two Firepower 1150s, each with a 100-user SSL VPN license. In a VPN load-balancing group, does the maximum total number of users allow 200 simultaneous sessions, or only 100? If we add a third device later with a 100-user license, can we now support 300 simultaneous sessions?

A. With VPN load balancing, all devices are active, so the maximum number of sessions that your group can support is the total of the number of sessions for each of the devices in the group, in this case 300.

Licensing for VPN Load Balancing

VPN load balancing has the following licensing requirements:

- An active 3DES/AES license.

  ASA checks for the existence of this crypto license before enabling VPN load balancing. If it does not detect an active 3DES or AES license, the ASA prevents the enabling of VPN load balancing and also

prevents internal configuration of 3DES by the VPN load-balancing system unless the license permits this usage.

- A valid Security Plus license for this feature activated on your firewall.
- You must have enough of these Security Plus licenses in your Smart account to be compliant.

Prerequisites for VPN Load Balancing

Also refer to the Guidelines and Limitations for VPN Load Balancing, on page 45.

- VPN load balancing is disabled by default. You must explicitly enable VPN load balancing.
- You must have first configured the public (outside) and private (inside) interfaces. Subsequent references in this section use the names outside and inside.

  To do so, go to **Configuration > Device Setup > Interface Settings > Interfaces**.
- You must have previously configured the interface to which the virtual IP address refers. Establish a common virtual IP address, UDP port (if necessary), and IPsec shared secret for the group.
- All devices that participate in a group must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.
- To use VPN load-balancing group encryption, first enable IKEv1 on the inside interface using the **crypto ikev1 enable** command, with the inside interface specified; otherwise you will get an error message when you try to configure VPN load-balancing group encryption.
- The Local CA feature is not supported if you use Active/Active stateful failover or VPN load-balancing. The Local CA cannot be subordinate to another CA; it can act only as the Root CA.

Guidelines and Limitations for VPN Load Balancing

Eligible Clients

VPN Load balancing is effective only on remote sessions initiated with the following clients:

- Secure Client (Release 3.0 and later)
- ASA 5505 (when acting as an Easy VPN client)
- Firepower 1010 (when acting as an Easy VPN client)
- IOS EZVPN Client devices supporting IKE-redirect (IOS 831/871)

Client Considerations

VPN load balancing works with IPsec clients and SSL VPN client sessions. All other VPN connection types (L2TP, PPTP, L2TP/IPsec), including LAN-to-LAN, can connect to an ASA on which VPN load balancing is enabled, but they cannot participate in VPN load balancing.

When multiple ASA nodes are grouped for load balancing, and using Group URLs is desired for AnyConnect Client connections, the individual ASA nodes must:

- Configure each remote access connection profile with a Group URL for each VPN load-balancing virtual address (IPv4 and IPv6).
- Configure a Group URL for this node's VPN load-balancing public address.

Load Balancing Group

- ASA supports 10 devices per VPN load balancing group.
- UCAPL mode does not support VPN load balancing, even when encryption is disabled. In UCAPL mode, use IKEv2 for secure tunnel establishment.

Context Mode

VPN load balancing is not supported in multiple context mode.

FIPS

Cluster encryption not supported with FIPS.

Certificate Verification

When performing certificate verification for VPN load balancing with AnyConnect Client, and the connection is redirected by an IP address, the client does all of its name checking through this IP address. Make sure the redirection IP address is listed in the certificates common name or the subject alt name. If the IP address is not present in these fields, then the certificate will be deemed untrusted.

Following the guidelines defined in RFC 2818, if a **subject alt name** is included in the certificate, we only use the **subject alt name** for name checks, and we ignore the common name. Make sure that the IP address of the server presenting the certificate is defined in the **subject alt name** of the certificate.

For a standalone ASA, the IP address is the IP of that ASA. In a VPN load-balancing group situation, it depends on the certificate configuration. If the group uses one certificate, then the certificate should have SAN extensions for the virtual IP address and group FQDN and should contain Subject Alternative Name extensions that have each ASA's IP and FQDN. If the group uses multiple certificates, then the certificate for each ASA should have SAN extensions for the virtual IP, group FQDN, and the individual ASA's IP address and FQDN.

Geographical VPN Load Balancing

In a VPN load balancing environment where the DNS resolutions are being changed at regular intervals, you must carefully consider how to set the time to live (TTL) value. For the DNS load balance configuration to work successfully with AnyConnect Client, the ASA name-to-address mapping must remain the same from the time the ASA is selected until the tunnel is fully established. If too much time passes before the credentials are entered, the lookup restarts and a different IP address may become the resolved address. If the DNS mapping changes to a different ASA before the credentials are entered, the VPN tunnel fails.

Geographical load balancing for VPN often uses a Cisco Global Site Selector (GSS). The GSS uses DNS for the load balancing, and the time to live (TTL) value for DNS resolution is defaulted to 20 seconds. You can significantly decrease the likelihood of connection failures if you increase the TTL value on the GSS. Increasing to a much higher value allows ample time for the authentication phase when the user is entering credentials and establishing the tunnel.

To increase the time for entering credentials, you may also consider disabling Connect on Start Up.

IKE/IPSec Security Associations

Cluster encryption sessions do not sync to standby in a VPN load balancer topology.

Configuring VPN Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called VPN load balancing, which directs session traffic to the least loaded device, thereby distributing the load among all devices. VPN load balancing makes efficient use of system resources and provides increased performance and system availability.

To use VPN load balancing, do the following on each device in the group:

- Configure the VPN load-balancing group by establishing common VPN load-balancing group attributes. This includes a virtual IP address, UDP port (if necessary), and IPsec shared secret for the group. All participants in the group must have an identical group configuration, except for the device priority within the group.
- Configure the participating device by enabling VPN load balancing on the device and defining device-specific properties, such as its public and private addresses. These values vary from device to device.

Configure VPN Load Balancing with the High Availability and Scalability Wizard

Procedure

Step 1 Choose **Wizards** > **High Availability and Scalability**.

Step 2 In the Configuration Type screen, click **Configure VPN Cluster Load Balancing**, and click **Next**.

Step 3 Choose the single IP address that represents the entire VPN load-balancing group. Specify an IP address that is within the public subnet address range shared by all the ASAs in the group.

Step 4 Specify the UDP port for the VPN load-balancing group in which this device is participating. The default value is 9023. If another application is using this port, enter the UDP destination port number that you want to use for VPN load balancing.

Step 5 To enable IPsec encryption and ensure that all VPN load-balancing information communicated between the devices is encrypted, check the **Enable IPsec Encryption** check box.

Step 6 Specify and verify the **IPsec shared secret**. The value that you enter appears as consecutive asterisk characters.

Step 7 Specify the priority assigned to this device within the group. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the group director, either at startup or when an existing director fails. The higher the priority set (for example, 10), the more likely that this device will become the director.

Note
If the devices in the VPN load-balancing group are powered up at different times, the first device to be powered up assumes the role of director. Each device in the group checks when it is powered up to ensure that the group has a director. If none exists, that device assumes the role. Devices powered up and added to the group later become group members. If all the devices in the group are powered up simultaneously, the device with the highest priority setting becomes the director. If two or more devices in the group are powered up simultaneously, and both have the highest priority setting, the one with the lowest IP address becomes the director.

Step 8 Choose **Public Interface of This Device**.

Step 9 Choose the **Private Interface of This Device**.

Step 10 Check the **Send FQDN to client instead of an IP address when redirecting** check box to have the director send a fully qualified domain name using the host and domain name of the device instead of the outside IP address when redirecting VPN client connections to that device.

Step 11 Click **Next**. Review your configuration in the Summary screen.

Step 12 Click **Finish**.

The VPN load-balancing group configuration is sent to the ASA.

What to do next

When multiple ASA nodes are grouped for load balancing, and using Group URLs is desired for AnyConnect Client connections, the individual ASA nodes must:

- Configure each remote access connection profile with a Group URL for each VPN load-balancing virtual address (IPv4 and IPv6).
- Configure a Group URL for this node's VPN load-balancing public address.

Group URLs are configured in the **Configuration > Remote Access VPN > Network (Client) Access >** AnyConnect Client **Connection Profiles >** *connection profile name* > **Add or Edit > Advanced > Group Alias / Group URL** pane.

Configure VPN Load Balancing (Without the Wizard)

Procedure

Step 1 Select **Configuration** > **Remote Access VPN** > **Load Balancing.**

Step 2 Check **Participate in Load Balancing** to indicate that this ASA is a participant in the load-balancing cluster

You must enable load balancing in this way on every ASA participating in load balancing.

Step 3 Configure the following fields in the **VPN Cluster Configuration** area. These values must be the same for the entire virtual cluster. All servers in the cluster must have an identical cluster configuration.

- **Cluster IPv4 Address**—Specifies the single IPv4 address that represents the entire IPv4 virtual cluster. Choose an IP address that is within the public subnet address range shared by all the ASAs in the virtual cluster.
  - **UDP Port**—Specifies the UDP port for the virtual cluster in which this device is participating. The default value is 9023. If another application is using this port, enter the UDP destination port number you want to use for load balancing.
- **Cluster IPv6 Address**—Specifies the single IPv6 address that represents the entire IPv6 virtual cluster. Choose an IP address that is within the public subnet address range shared by all the ASAs in the virtual cluster. Clients with IPv6 addresses can make AnyConnect Client connections through the ASA cluster's public-facing IPv6 address or through a GSS server. Likewise, clients with IPv6 addresses can make

AnyConnect Client VPN connections through the ASA cluster's public-facing IPv4 address or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.

Note
In the Cluster IPv4 Address and Cluster IPv6 Address fields, you can also specify the fully qualified domain name of the virtual cluster, provided that you have a DNS server group configured with at least one DNS server, and DNS lookup is enabled on one of the ASA's interfaces.

- **Enable IPsec Encryption**—Enables or disables IPsec encryption. If you check this box, you must also specify and verify a shared secret. The ASAs in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec. To ensure that all load-balancing information communicated between the devices is encrypted, check this box.
- **IPsec Shared Secret**—Specifies the shared secret between IPsec peers when you have enabled IPsec encryption. The value you enter in the box appears as consecutive asterisk characters.
- **Verify Secret**—Re-enter the shared secret. Confirms the shared secret value entered in the IPsec Shared Secret box.

Step 4 Configure the fields in the **VPN Server Configuration** area for a specific ASA:

- **Public Interface**—Specifies the name or IP address of the public interface for this device.
- **Private Interface**—Specifies the name or IP address of the private interface for this device.
- **Priority**—Specifies the priority assigned to this device within the cluster. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority (for example, 10), the more likely this device becomes the virtual cluster master.

  Note
  If the devices in the virtual cluster are powered up at different times, the first device to be powered up assumes the role of virtual cluster master. Because every virtual cluster requires a master, each device in the virtual cluster checks when it is powered-up to ensure that the cluster has a virtual master. If none exists, that device takes on the role. Devices powered up and added to the cluster later become backup devices. If all the devices in the virtual cluster are powered up simultaneously, the device with the highest priority setting becomes the virtual cluster master. If two or more devices in the virtual cluster are powered up simultaneously, and both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

- **NAT Assigned IPv4 Address**—Specifies the IP address that this device's IP address is translated to by NAT. If NAT is not being used (or if the device is not behind a firewall using NAT), leave the field blank.
- NAT Assigned IPv6 Address—Specifies the IP address that this device's IP address is translated to by NAT. If NAT is not being used (or if the device is not behind a firewall using NAT), leave the field blank.
- **Send FQDN to client**—Check this check box to cause the VPN cluster master to send a fully qualified domain name using the host and domain name of the cluster device instead of the outside IP address when redirecting VPN client connections to that cluster device.

  By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a backup device.

As a VPN cluster master, this ASA can send a fully qualified domain name (FQDN), using reverse DNS lookup, of a cluster device (another ASA in the cluster), instead of its outside IP address, when redirecting VPN client connections to that cluster device.

All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

Note
When using IPv6 and sending FQDNS down to client, those names must be resolvable by the ASA via DNS.

What to do next

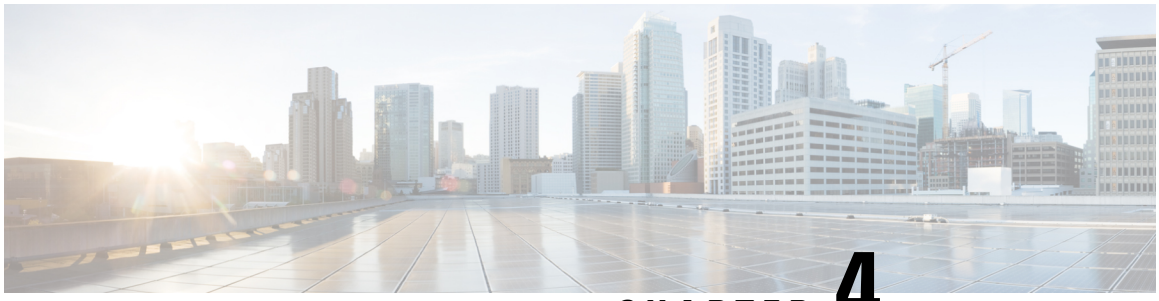
When multiple ASA nodes are clustered for load balancing, and using Group URLs is desired for AnyConnect Client connections, the individual ASA nodes must:

- Configure each remote access connection profile with a Group URL for each load balancing virtual cluster address (IPv4 and IPv6).
- Configure a Group URL for this node's VPN Load Balancing public address.

Group URLs are configured in the **Configuration > Remote Access VPN > Network (Client) Access >** AnyConnect Client **Connection Profiles >** *connection profile name* > **Add or Edit > Advanced > Group Alias / Group URL** pane.

Feature History for VPN Load Balancing

Feature Name	Releases	Feature Information
VPN Load balancing with SAML	9.17(1)	ASA now supports VPN load balancing with SAML authentication.
VPN Load balancing	7.2(1)	This feature was introduced.



CHAPTER 4

General VPN Setup

- System Options, on page 51
- Configure Maximum VPN Sessions, on page 53
- Configure DTLS, on page 53
- Configure DNS Server Groups, on page 54
- Configure the Pool of Cryptographic Cores, on page 55
- Client Addressing for SSL VPN Connections, on page 55
- Group Policies, on page 56
- Connection Profiles, on page 91
- IKEv1 Connection Profiles, on page 108
- **IKEv2 Connection Profiles**, on page 113
- Mapping Certificates to IPsec or SSL VPN Connection Profiles, on page 115
- Site-to-Site Connection Profiles, on page 119
- AnyConnect VPN module of Cisco Secure Client Image, on page 125
- AnyConnect Client External Browser SAML Package, on page 126
- Configure AnyConnect Client VPN Connections, on page 128
- AnyConnect Client HostScan, on page 135
- Install or Upgrade HostScan/Secure Firewall Posture, on page 135
- Configure Posture Settings, on page 136
- Uninstall HostScan/Secure Firewall Posture, on page 137
- Assign AnyConnect Client Feature Modules to Group Policies, on page 137
- HostScan/Secure Firewall Posture Related Documentation, on page 139
- Secure Client Solution, on page 139
- AnyConnect Client Customization and Localization, on page 141
- AnyConnect Client Custom Attributes, on page 143
- IPsec VPN Client Software , on page 146
- Zone Labs Integrity Server, on page 146
- ISE Policy Enforcement, on page 147

System Options

The **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options** pane (also reached using **Configuration > Site-to-Site VPN > Advanced > System Options)** lets you configure features specific to IPsec and VPN sessions on the ASA.

- Limit the maximum number of active IPsec VPN sessions—Enables or disables limiting the maximum number of active IPsec VPN sessions. The range depends on the hardware platform and the software license.
  - Maximum IPsec Sessions—Specifies the maximum number of active IPsec VPN sessions allowed. This field is active only when you choose the preceding check box to limit the maximum number of active IPsec VPN sessions.
- L2TP Tunnel Keep-alive Timeout—Specifies the frequency, in seconds, of keepalive messages. The range is 10 through 300 seconds. The default is 60 seconds. This is an advanced system option for Network (Client) Access only.
- Reclassify existing flows when VPN tunnels establish
- Preserve stateful VPN flows when the tunnel drops—Enables or disables preserving IPsec tunneled flows in Network-Extension Mode (NEM). With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout dialog box, data continues flowing successfully because the security appliance still has access to the state information. This option is disabled by default.



Note Tunneled TCP flows are not dropped, so they rely on the TCP timeout for cleanup. However, if the timeout is disabled for a particular tunneled flow, that flow remains in the system until being cleared manually or by other means (for example, by a TCP RST from the peer).

- IPsec Security Association Lifetime—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
  - **Time**—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
  - **Traffic Volume**—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires, or check unlimited. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Enable PMTU (Path Maximum Transmission Unit) Aging—Allows an administrator to enable PMTU aging.
  - Interval to Reset PMTU of an SA (Security Association)—Enter the number of seconds at which the PMTU value is reset to its original value.
- Enable inbound IPsec sessions to bypass interface access-lists. Group policy and per-user authorization ACLs still apply to the traffic—By default, the ASA allows VPN traffic to terminate on an ASA interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an access rule. When this option is checked, you also do not need an access rule for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the ASA performance without any security risks. (Group policy and per-user authorization ACLs still apply to the traffic.)

  You can require an access rule to apply to the local IP addresses by unchecking this option. The access rule applies to the local IP address, and not to the original client IP address used before the VPN packet was decrypted.

- Permit communication between VPN peers connected to the same interface—Enables or disables this feature.

  You can also redirect incoming client VPN traffic back out through the same interface unencrypted as well as encrypted. If you send VPN traffic back out through the same interface unencrypted, you should enable NAT for the interface so that publicly routable addresses replace your private IP addresses (unless you already use public IP addresses in your local IP address pool).

- Compression Settings—Specifies the features for which you want to enable compression: WebVPN, and SSL VPN Client. Compression is enabled by default.

Configure Maximum VPN Sessions

To specify the maximum allowed number of VPN sessions or AnyConnect Client VPN sessions, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Advanced** > **Maximum VPN Sessions**.

Step 2 In the **Maximum** AnyConnect Client **Sessions** field, enter the maximum number of sessions allowed.

Valid values range from 1 to the maximum number of sessions that are allowed by your license.

Step 3 In the **Maximum Other VPN Sessions** field, enter the maximum number of VPN sessions allowed, which includes Cisco VPN client (IPsec IKEv1) and LAN-to-LAN VPN sessions.

Valid values range from 1 to the maximum number of sessions that are allowed by your license.

Step 4 Click **Apply**.

Configure DTLS

Datagram Transport Layer Security (DTLS) allows the AnyConnect Client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Before you begin

See, SSL Settings, on page 209to configure DTLS on this headend, and which version of DTLS is used.

In order for DTLS to fall back to a TLS connection, Dead Peer Detection (DPD) must be enabled. If you do not enable DPD, and the DTLS connection experiences a problem, the connection terminates instead of falling back to TLS. For more information on DPD, see Internal Group Policy, AnyConnect Client, Dead Peer Detection, on page 82.

Procedure

Step 1 Specify DTLS options for AnyConnect Client VPN connections:

a) Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles , Access Interfaces** section.

b) In the **Interface** table, in the row for the interface you are configuring for AnyConnect Client connections, check the protocols you want to enable on the interface.

- When you check or enable **SSL Access / Allow Access**, **Enable DTLS** is checked or enabled by default.
- To disable DTLS, uncheck **Enable DTLS**. SSL VPN connections will connect with an SSL VPN tunnel only.

c) Choose **Port Settings** to configure **SSL Ports**.

- **HTTPS Port**—The port to enable for HTTPS (browser-based) SSL connections. The range is 1-65535. The default is port 443.
- **DTLS Port**—The UDP port to enable for DTLS connections. The range is 1-65535. The default is port 443.

Step 2 Specify DTLS options for specific group policies.

a) Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, then **Add/Edit > Advanced >** AnyConnect Client.

b) Choose Inherit (default), Enable or Disable for **Datagram Transport Layer Security (DTLS)**.

c) Choose Inherit (default), Enable or Disable for **DTLS Compression**, which configures compression for DTLS.

Configure DNS Server Groups

The **Configuration > Remote Access VPN > DNS** dialog box displays the configured DNS servers in a table, including the server group name, servers, timeout in seconds, number of retries allowed, and domain name. You can add, edit, or delete DNS server groups in this dialog box.

- Add or Edit—Opens the Add or Edit DNS Server Group dialog box. Help for which exists elsewhere
- Delete—Removes the selected row from the table. There is no confirmation or undo.
- DNS Server Group—Selects the server to use as the DNS server group for this connection. The default is DefaultDNS.
- Manage—Opens the Configure DNS Server Groups dialog box.

Configure the Pool of Cryptographic Cores

You can change the allocation of cryptographic cores on Symmetric Multi-Processing (SMP) platforms to increase the throughput of AnyConnect Client TLS/DTLS traffic. These changes can accelerate the SSL VPN datapath and provide customer-visible performance gains in AnyConnect Client, smart tunnels, and port forwarding. These steps describe configuring the pool of cryptographic cores in either single or multiple context mode.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Advanced** > **Crypto Engine**.

Step 2 From the Accelerator Bias drop-down list, specify how to allocate crypto accelerator processors:

Note
This field only shows up if the feature is available on the device.

- **balanced**—Equally distributes cryptography hardware resources (Admin/SSL and IPsec cores).
- **ipsec**—Allocates cryptography hardware resources to favor IPsec (includes SRTP encrypted voice traffic).
- **ssl**—Allocates cryptography hardware resources to favor Admin/SSL. Use this bias when you support SSL-based AnyConnect Client remote access VPN sessions.

Step 3 Click **Apply**.

Client Addressing for SSL VPN Connections

Use this dialog box to specify the global client address assignment policy and to configure interface-specific address pools. You can also add, edit, or delete interface-specific address pools using this dialog box. The table at the bottom of the dialog box lists the configured interface-specific address pools.

- Global Client Address Assignment Policy—Configures a policy that affects all IPsec and SSL VPN Client connections (including AnyConnect Client connections). The ASA uses the selected sources in order, until it finds an address:
  - Use authentication server—Specifies that the ASA should attempt to use the authentication server as the source for a client address.
  - Use DHCP—Specifies that the ASA should attempt to use DHCP as the source for a client address.
  - Use address pool—Specifies that the ASA should attempt to use address pools as the source for a client address.
- Interface-Specific IPv4 Address Pools—Lists the configured interface-specific address pools.
- Interface-Specific IPv6 Address Pools—Lists the configured interface-specific address pools.

- Add—Opens the Assign Address Pools to Interface dialog box, on which you can choose an interface and choose an address pool to assign.
- Edit—Opens the Assign Address Pools to Interface dialog box with the interface and address pool fields filled in.
- Delete—Deletes the selected interface-specific address pool. There is no confirmation or undo.

Assign Address Pools to Interface

Use this dialog box to choose an interface and assign one or more address pools to that interface.

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, in which you can choose one or more address pools to assign to this interface. Your selection appears in the Address Pools field of the Assign Address Pools to Interface dialog box.

Select Address Pools

The Select Address Pools dialog box shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you add, edit, or delete entries from that list.

- Add—Opens the Add IP Pool dialog box, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool dialog box, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments.

Add or Edit an IP Address Pool

Configures or modifies an IP address pool.

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

Group Policies

A group policy is a collection of user-oriented attribute/value pairs stored either internally on the ASA or externally on a RADIUS or LDAP server. A group policy assigns attributes to a client when the establish a VPN connection. By default, VPN users have no group policy association. The group policy information is used by VPN connection profiles (tunnel groups) and user accounts.

The ASA supplies a default group policy named DfltGrpPolicy. The default group parameters are those that are most likely to be common across all groups and users, which can help streamline the configuration task. New groups can "inherit" parameters from this default group, and users can "inherit" parameters from their group or the default group. You can override these parameters as you configure groups and users.

You can configure internal and external group policies. An internal group policy is stored locally, and an external group policy is stored externally on a RADIUS or LDAP server.

In the Group Policy dialog boxes, you configure the following kinds of parameters:

- General attributes: Name, banner, address pools, protocols, filtering, and connection settings.
- Servers: DNS and WINS servers, DHCP scope, and default domain name.
- Advanced attributes: Split tunneling, IE browser proxy, and AnyConnect Client, and IPsec client.

Before configuring these parameters, you should configure:

- Access hours (General | More Options | Access Hours).
- Filters (General| More Options | Filters).
- IPsec Security Associations (Configuration | Policy Management | Traffic Management | Security Associations).
- Network lists for filtering and split tunneling (Configuration | Policy Management | Traffic Management | Network Lists).
- User authentication servers and the internal authentication server (Configuration | System | Servers | Authentication).

You can configure these types of group policies:

- External Group Policies, on page 58—An external group policy points the ASA to the RADIUS or LDAP server to retrieve much of the policy information that would otherwise be configured in an internal group policy. External group policies are configured the same way for Network (Client) Access VPN connections and Site-to-Site VPN connections.
- Internal Group Policies, on page 60—These connections are initiated by a VPN client installed on the endpoint. The Secure Client and Cisco VPN IPsec client are examples of VPN clients. After the VPN client is authenticated, remote users can access corporate networks or applications as if they were on-site. The data traffic between remote users and the corporate network is secured by being encrypted when going through the Internet.
- AnyConnect Client Internal Group Policies, on page 65
- Site-to-Site Internal Group Policies, on page 88

Group Policy Pane Fields

The Configuration > Remote Access VPN > Network (Client) Access > Group Policies pane in ASDM lists the currently configured group policies. The Add, Edit, and Delete buttons to help you manage VPN group policies, as described below.

- Add—Offers a drop-down list on which you can choose whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy. Clicking Add opens the Add Internal Group Policy dialog box or the Add External Group Policy dialog box, which let you

add a new group policy to the list. This dialog box includes three menu sections. Click each menu item to display its parameters. As you move from item to item, ASDM retains your settings. When you have finished setting parameters on all menu sections, click **Apply** or **Cancel**.

- Edit—Displays the Edit Group Policy dialog box, which lets you modify an existing group policy.
- Delete—Lets you remove a AAA group policy from the list. There is no confirmation or undo.
- Assign—Lets you assign a group policy to one ore more connection profiles.
- Name—Lists the name of the currently configured group policies.
- Type—Lists the type of each currently configured group policy.
- Tunneling Protocol—Lists the tunneling protocol that each currently configured group policy uses.
- Connection Profiles/Users Assigned to—Lists the connection profiles and users configured directly on the ASA that are associated with this group policy.

External Group Policies

External group policies retrieve attribute values authorization and authentication from an external server. The group policy identifies the RADIUS or LDAP server group that the ASA can query for attributes, and specifies the password to use when retrieving those attributes.

External group names on the ASA refer to user names on the RADIUS server. In other words, if you configure external group X on the ASA, the RADIUS server sees the query as an authentication request for user X. So external groups are really just user accounts on the RADIUS server that have special meaning to the ASA. If your external group attributes exist in the same RADIUS server as the users that you plan to authenticate, there must be no name duplication between them.

Before you configure the ASA to use an external server, you must configure that server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users. Follow the instructions in “External Server for Authorization and Authentication” to configure your external server.

These RADIUS configurations include RADIUS with LOCAL authentication, RADIUS with Active Directory/Kerberos Windows DC, RADIUS with NT/4.0 Domain, and RADIUS with LDAP.

External Group Policy Fields

- Name—Identifies the group policy to be added or changed. For Edit External Group Policy, this field is display-only.
- Server Group—Lists the available server groups to which to apply this policy.
- New—Opens a dialog box that lets you choose whether to create a new RADIUS server group or a new LDAP server group. Either of these options opens the Add AAA Server Group dialog box.
- Password—Specifies the password for this server group policy.

For information about creating and configuring AAA servers, see the *Cisco ASA Series General Operations ASDM Configuration Guide*, the *AAA Servers and Local Database* chapter.

Password Management with AAA Servers

The ASA supports password management for the RADIUS and LDAP protocols. It supports the "password-expire-in-days" option only for LDAP. The other parameters are valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.



Note Some RADIUS servers that support MS-CHAP currently do not support MS-CHAPv2. This feature requires MS-CHAPv2, so check with your vendor.

The ASA generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN client
- IPsec VPN client
- IPsec IKEv2 clients

Password management is *not* supported for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. Some RADIUS servers, for example, Cisco ACS, can proxy the authentication request to another authentication server. However, from the perspective of the ASA, it is communicating only to a RADIUS server.



Note For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.

Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Password Support with AnyConnect Client

The ASA supports the following password management features for AnyConnect Client:

- Password expiration notice, when the user tries to connect.
- Password expiration reminders, before the password has expired.
- Password expiration override. The ASA ignores password expiration notices from the AAA server, and authorizes the user's connection.

When password management is configured, the ASA notifies remote users when they try to log in that their current password has expired, or is about to expire. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using the old password, and change the password later.

The AnyConnect Client cannot initiate password change, it can only respond to a change request from the AAA server through the ASA. The AAA server must be a RADIUS server proxying to AD, or an LDAP server.

The ASA does not support password management under the following conditions:

- when using LOCAL (internal) authentication
- when using LDAP authorization
- when using RADIUS authentication only, and when the users reside on the RADIUS server database

Setting password expiration override tells the ASA to ignore account-disabled indications from a AAA server. This can be a security risk. For example, you may not want to change the Administrators' password.

Enabling password management causes the ASA to send MS-CHAPv2 authentication requests to the AAA server.

Internal Group Policies

Internal Group Policy, General Attributes

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** pane, the Add or Edit Group Policy dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields in this dialog box, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all of the attributes in this dialog box.

You configure the general attributes of an internal group policy in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General.** The following attributes apply to SSL VPN and IPsec sessions. Thus, some attributes are present for one type of session, but not the other.

- **Name**—Specifies the name of this group policy, up to 64 characters; spaces are allowed. For the Edit function, this field is read-only.
- **Banner**—Specifies the banner text to present to users at login. The length can be up to 4000 characters. There is no default value.

  The IPsec VPN client supports full HTML for the banner. However, the clientless portal and the AnyConnect Client support partial HTML. To ensure the banner displays properly to remote users, follow these guidelines:

  - For IPsec client users, use the /n tag.
  - For AnyConnect Client users, use the <BR> tag.

- **SCEP forwarding URL**—Address of the CA, required when SCEP Proxy is configured in the client profile.
- **Address Pools**—Specifies the name of one or more IPv4 address pools to use for this group policy. If the Inherit check box is checked, the group policy uses the IPv4 address pool specified in the Default Group Policy. See for information on adding or editing an IPv4 address pool.



Note You can specify both an IPv4 and an IPv6 address pool for an internal group policy.

Select—Uncheck the Inherit checkbox to activate this button. Click **Select** to open the Address Pools dialog box, which shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you choose, add, edit, delete, and assign entries from that list.

- **IPv6 Address Pools**—Specifies the name of one or more IPv6 address pools to use for this group policy.

  Select—Uncheck the Inherit checkbox to activate this button. Click **Select** to open the Select Address Pools dialog box, as previously described. See for information on adding or editing an IPv6 address pool.

- **More Options**—Click the down arrows at the right of the field to display additional configurable options for this group policy.
- **Tunneling Protocols**—Specifies the tunneling protocols that this group can use. Users can use only the selected protocols. The choices are as follows:
  - **Clientless SSL VPN**—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to an ASA; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
  - **SSL VPN Client**—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client. If you are using the AnyConnect Client, you must choose this protocol for Mobile User Security (MUS) to be supported.
  - **IPsec IKEv1**—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both Site-to-Site (peer-to-peer) connections and Cisco VPN client-to-LAN connections can use IPsec IKEv1.
  - **IPsec IKEv2**—Supported by the Secure Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
  - **L2TP over IPsec**—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.
- **Filter**—Specifies which access control list to use for an IPv4 or an IPv6 connection, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. Note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection. To configure filters and rules, click **Manage**.
- **NAC Policy**—Selects the name of a Network Admission Control policy to apply to this group policy. You can assign an optional NAC policy to each group policy. The default value is --None--.
- **Manage**—Opens the Configure NAC Policy dialog box. After configuring one or more NAC policies, the NAC policy names appear as options in the drop-down list next to the NAC Policy attribute.
- **Access Hours**—Selects the name of an existing access hours policy, if any, applied to this user or create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not checked, the default value is --Unrestricted--. Click **Manage** to open the Browse Time Range dialog box, in which you can add, edit, or delete a time range.

- **Simultaneous Logins**—Specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.

Note While there is no maximum limit, allowing several simultaneous connections might compromise security and affect performance.

- **Restrict Access to VLAN**—(Optional) Also called "VLAN mapping," this parameter specifies the egress VLAN interface for sessions to which this group policy applies. The ASA forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using ACLs to filter traffic on a session. In addition to the default value (Unrestricted), the drop-down list shows only the VLANs that are configured in this ASA.

Note This feature works for HTTP connections, but not for FTP and CIFS.

- **Connection Profile (Tunnel Group) Lock**—This parameter permits remote VPN access only with the selected connection profile (tunnel group), and prevents access with a different connection profile. The default inherited value is None.
- **Maximum Connect Time**—If the **Inherit** check box is not checked, this parameter sets the maximum user connection time in minutes.

  At the end of this time, the system terminates the connection. The minimum is 1minute, and the maximum is 35791394 minutes. To allow unlimited connection time, check **Unlimited** (default).
- **Idle Timeout**—If the **Inherit** check box is not checked, this parameter sets the idle timeout in minutes.

  If there is no communication activity on the connection in this period, the system terminates the connection. The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.
- **Security Group Tag (SGT)**—Enter the numerical value of the SGT tag that will be assigned to VPN users connecting with this group policy.
- **On smart card removal**—With the default option, Disconnect, the client tears down the connection if the smart card used for authentication is removed. Click **Keep the connection** if you do not want to require users to keep their smart cards in the computer for the duration of the connection.

  Smart card removal configuration only works on Microsoft Windows using RSA smart cards.
- **Disable Delete tunnel with no delay in Simultaneous Session preempt**—When a given user reaches the allowed **Simultaneous Logins** limit, the user's next login attempt requires the system to first delete the oldest session. This deletion can take a few seconds, which can prevent the user from establishing a new session immediately. Select this option to instruct the system to establish the new session without waiting for the deletion of the oldest session to complete.
- **Maximum Connection Time Alert Interval**—The interval of time before max connection time is reached that a message will be displayed to the user.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the session alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

- **Periodic Certificate Authentication Interval**—The interval of time in hours, before certificate authentication is redone periodically.

  If the **Inherit** check box is not checked, you can set the interval for performing periodic certificate verification. The range is between 1 and 168 hours, and the default is disabled. To allow unlimited verification, check Unlimited.

Configure Internal Group Policy, Server Attributes

Configure DNS servers, WINS servers and DHCP Scope in the Group Policy > Servers window. DNS and WINS servers are applied to full-tunnel clients (IPsec, AnyConnect Client, SVC, and L2TP/IPsec) only and are used for name resolution. DHCP scope is used when DHCP-address assignment is in place.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **Servers**.

Step 2 Unless you are editing the DefaultGroupPolicy, uncheck the DNS Servers **Inherit** checkbox and add the IPv4 or IPv6 addresses of the DNS servers you want this group to use. You can specify two IPv4 addresses and two IPv6 addresses.

If you specify more than one DNS server, the remote access client attempts to use the DNS servers in the order you specify in this field.

Changes you make here override the DNS setting configured on the ASDM in the **Configuration > Remote Access VPN > DNS** window for clients using this group policy.

Step 3 Uncheck the WINS Servers **Inherit** checkbox and enter the IP addresses of the primary and secondary WINS servers. The first IP address you specify is that of the primary WINS server. The second (optional) IP address you specify is that of the secondary WINS server. .

Step 4 Expand the **More Options** area by clicking the double down arrow in the More Options bar.

Step 5 Uncheck DHCP Scope **Inherit** and define the DHCP scope.

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the

DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

Step 6 If there is no default domain specified in the **Configuration** > **Remote Access VPN** > **DNS** window, you must specify the default domain in the **Default Domain** field. Use the domain name and top level domain for example, example.com.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Internal Group Policy, Browser Proxy

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > Browser Proxy

This dialog box configures attributes that will be pushed down to the client to reconfigure Microsoft Internet Explorer settings:

- Proxy Server Policy—Configures the Microsoft Internet Explorer browser proxy actions ("methods") for a client PC.
  - Do not modify client proxy settings—Leaves the HTTP browser proxy server setting in Internet Explorer unchanged for this client PC.
  - Do not use proxy—Disables the HTTP proxy setting in Internet Explorer for the client PC.
  - Select proxy server settings from the following—Enables the following check boxes for your selections: Auto detect proxy, Use proxy server settings given below, and Use proxy auto configuration (PAC) given below.
  - Auto detect proxy—Enables the use of automatic proxy server detection in Internet Explorer for the client PC.
  - Use proxy server settings specified below—Sets the HTTP proxy server setting in Internet Explorer to use the value configured in the Proxy Server Name or IP Address field.
  - Use proxy auto configuration (PAC) given below—Specifies the use of the file specified in the Proxy Auto Configuration (PAC) field as the source for auto configuration attributes.
- Proxy Server Settings—Configures the proxy server parameters for Microsoft clients using Microsoft Internet Explorer.
  - Server Address and Port—Specifies the IP address or name and the port of an Microsoft Internet Explorer server that is applied for this client PC.
  - Bypass Proxy Server for Local Addresses—Configures Microsoft Internet Explorer browser proxy local-bypass settings for a client PC. Click **Yes** to enable local bypass or **No** to disable local bypass.
  - Exception List—Lists the server names and IP addresses that you want to exclude from proxy server access. Enter the list of addresses that you do not want to have accessed through a proxy server. This list corresponds to the Exceptions list in the Proxy Settings dialog box in Internet Explorer.
- Proxy Auto Configuration Settings—The PAC URL specifies the URL of the auto-configuration file. This file tells the browser where to look for proxy information. To use the proxy auto-configuration (PAC) feature, the remote user must use the Cisco AnyConnect VPN client.

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.
- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the PAC URL field to specify the URL from which to retrieve the .pac file. Then the browser uses the .pac file to determine the proxy settings.

- Proxy Lockdown
  - Allow Proxy Lockdown for Client System - Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect Client VPN session. In addition, from Windows 10 version 1703 (or later), enabling this feature also hides the system proxy tab in Settings app for the duration of an AnyConnect Client VPN session. Disabling the feature leaves the display of the Connections tab in Microsoft Internet Explorer and Proxy tab in Settings app unchanged; the default setting for them can be to show or hide, depending on the user registry settings.



Note Hiding the system proxy tab in the Settings app for the duration of an AnyConnect Client VPN session needs AnyConnect version 4.7.03052 or later.

AnyConnect Client Internal Group Policies

Internal Group Policy, Advanced, AnyConnect Client

- Keep Installer on Client System—Enable to allow permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.
- Compression—Compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred.

- Datagram TLS—Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- Ignore Don't Defrag (DF) Bit—This feature allows the force fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel. An example use case is for servers in your network that do not respond correctly to TCP MSS negotiations.
- Client Bypass Protocol—The Client Protocol Bypass feature allows you to configure how the AnyConnect Client manages IPv4 traffic when ASA is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

  When the AnyConnect Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect Client connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear."

  For example, assume that the ASA assigns only an IPv4 address to an AnyConnect Client connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

  If establishing an IPsec tunnel (as opposed to an SSL connection), the ASA is not notified whether or not IPv6 is enabled on the client, so ASA always pushes down the client bypass protocol setting.

- FQDN of This Device—This information is used by the client after network roaming in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support roaming between networks of different IP protocols (such as IPv4 to IPv6).



Note You cannot use the ASA FQDN present in the AnyConnect Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

  If the device FQDN is not pushed to the client, the client tries to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name.

  If the device FQDN is not pushed by the ASA, the client cannot re-establish the VPN session after roaming between networks of different IP protocols.

- MTU—Adjusts the MTU size for SSL connections. Enter a value in bytes, from 256 to 1410 bytes. By default, the MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.
- Keepalive Messages—Enter a number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that a connection through a proxy, firewall, or NAT device

remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

- **Optional Client Modules to Download**—To minimize download time, the AnyConnect Client requests downloads (from the ASA) only of modules that it needs for each feature that it supports. You must specify the names of modules that enable other features. The AnyConnect Client includes the following modules (some earlier versions have fewer modules):
  - AnyConnect Client DART—The Diagnostic AnyConnect Client Reporting Tool (DART) captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
  - AnyConnect Client Network Access Manager—Formerly called the Cisco Secure Services Client, this module provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks.
  - AnyConnect Client SBL—Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect Client before the Windows login dialog box appears.
  - Secure Firewall Posture Module—Formerly called the Cisco Secure Desktop HostScan feature, the posture module is integrated into AnyConnect Client and provides AnyConnect Client the ability to gather credentials for posture assessment prior to creating a remote access connection to the ASA.
  - ISE Posture—Uses the OPSWAT v3 library to perform posture checks to assess an endpoint's compliance. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges.
  - AMP Enabler—Used as medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base.
  - Network Visibility Module—Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. The NVM collects the endpoint telemetry and logs both the flow data and the file reputation in the syslog and also exports the flow records to a collector (a third-party vendor), which performs the file analysis and provides a UI interface.
  - Umbrella Roaming Security Module—Provides DNS-layer security when no VPN is active. It provides a subscription to either Cisco Umbrella Roaming service or OpenDNS Umbrella services, which add Intelligent Proxy and IP-Layer Enforcement features. The Umbrella Security Roaming profile associates each deployment with the corresponding service and automatically enables the corresponding protection level (whether content filtering, multiple policies, robust reporting, active directory integration, or basic DNS-layer security).

- Always-On VPN—Determine if the always-on VPN flag setting in the AnyConnect Client service profile is disabled or if the AnyConnect Client service profile setting should be used. The always-on VPN feature lets AnyConnnect automatically establish a VPN session after the user logs onto a computer. The VPN session remains up until the user logs off the computer. If the physical connection is lost, the session remains up, and AnyConnect Client continually attempts to reestablish the physical connection with the adaptive security appliance to resume the VPN session.

  Always-on VPN permits the enforcement of corporate policies to protect the device from security threats. You can use it to help ensure AnyConnect Client establishes a VPN session whenever the endpoint is

not in a trusted network. If enabled, a policy is configured to determine how network connectivity is managed in the absence of a connection.

Note Always-On VPN requires an AnyConnect Client release that supports Secure Client features.

- Client Profiles to Download—A profile is a group of configuration parameters that the AnyConnect Client uses to configure VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, and Umbrella Roaming Security module settings. Click **Add** to launch the Select AnyConnect Client Profiles window where you can specify previously-created profiles for this group policy.

Configure Split-Tunneling for AnyConnect Client Traffic

Split tunneling directs some of the AnyConnect Client network traffic through the VPN tunnel (encrypted) and other network traffic outside the VPN tunnel (unencrypted or “in the clear”).

Split tunneling is configured by creating a split tunneling policy, configuring an access control list for that policy, and adding the split tunnel policy to a group policy. When the group policy is sent to the client, that client uses the ACLs in the split tunneling policy to decide where to direct network traffic.

Note Split tunneling is a traffic management feature, not a security feature. For optimum security, we recommend that you do not enable split tunneling.

For Windows clients, firewall rules from the ASA are evaluated first, then the ones on the client. For Mac OS X, the firewall and filter rules on the client are not used. For Linux systems, starting with AnyConnect version 3.1.05149, you can configure AnyConnect Client to evaluate the client's firewall and filter rules, by adding a custom attribute named circumvent-host-filtering to a group profile, and setting it to true.

When you create access lists:

- You can specify both IPv4 and IPv6 addresses in an access control list.
- If you use a standard ACL, only one address or network is used.
- If you use extended ACLs, the source network is the split-tunneling network. The destination network is ignored.
- Access lists configured with any or with a split include or exclude of 0.0.0.0/0.0.0.0 or ::/0 will not be sent to the client. To send all traffic over the tunnel, choose **Tunnel All Networks** for the split-tunnel **Policy**.
- Address 0.0.0.0/255.255.255.255 or ::/128 is sent to the client only when the split-tunnel policy is **Exclude Network List Below**. This configuration tells the client not to tunnel traffic destined for any local subnets.
- AnyConnect Client passes traffic to all sites specified in the split tunneling policy, and to all sites that fall within the same subnet as the IP address assigned by the ASA. For example, if the IP address assigned by the ASA is 10.1.1.1 with a mask of 255.0.0.0, the endpoint device passes all traffic destined to 10.0.0.0/8, regardless of the split tunneling policy. Therefore, use a netmask for the assigned IP address that properly references the expected local subnet.

Before you begin

- You must create an access list with the appropriate ACEs.
- If you created a split tunnel policy for IPv4 networks and another for IPv6 networks, then the network list you specify is used for both protocols. So, the network list should contain access control entries (ACEs) for both IPv4 and IPv6 traffic. If you have not created these ACLs, see the general operations configuration guide.

In the following procedure, in all cases where there is an Inherit checkbox next to a field, leaving the Inherit check box checked means that the group policy you are configuring uses the same values for that field as the default group policy. Unchecking Inherit lets you specify new values specific to your group policy.

Procedure

Step 1 Connect to the ASA using ASDM and navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Click **Add** to add a new group policy or choose an existing group policy and click **Edit**.

Step 3 Select **Advanced** > **Split Tunneling**.

Step 4 In the **DNS Names** field, enter the domain names that are to be resolved by AnyConnect Client via the tunnel. These names correspond to hosts in the private network. If split-include tunneling is configured, the network list must include the specified DNS servers. You can enter a full qualified domain name, IPv4 or IPv6 address in the field.

A dynamic split tunneling domain name requires at least one domain name label besides the top level domain. Because dynamic split tunneling is meant to target flows matching specific domain names, specifying just a top level domain (such as *org*) is unacceptable. You are required to enter the top level domain and at least one domain name label (such as *domain.org)*.

Step 5 To disable split tunneling, click **Yes** to enable **Send All DNS Lookups Through Tunnel**. This option ensures that DNS traffic is not leaked to the physical adapter; it disallows traffic in the clear. If DNS resolution fails, the address remains unresolved, and the AnyConnect Client does not try to resolve the address outside the VPN.

To enable split tunneling, choose **No** (the default). This setting tells the client to send DNS queries over the tunnel according to the split tunnel policy.

Step 6 To configure split-tunneling, uncheck the **Inherit** check box and choose a split-tunneling policy. If you do not uncheck **Inherit**, your group policy uses the split tunneling settings defined in the default group policy, **DfltGrpPolicy**. The default split tunneling policy setting in the default group policy is to Tunnel All Networks.

To define the split tunneling policy, chose from the drop-downs **Policy** and **IPv6 Policy**. The Policy field defines the split tunneling policy for IPv4 network traffic. The IPv6 Policy field selects the split tunneling policy for IPv6 network traffic. Other than that difference, these fields have the same purpose.

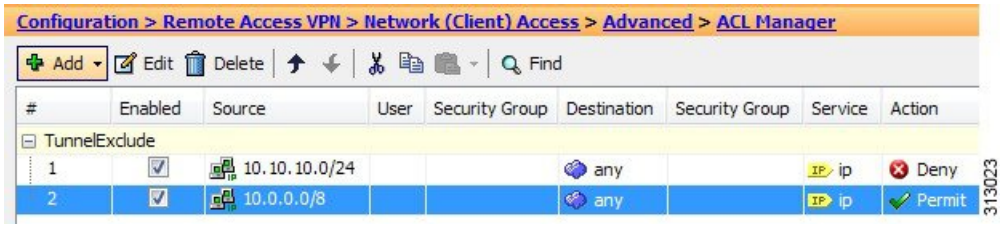
Unchecking **Inherit** allows you to choose one of these policy options:

- **Exclude Network List Below**—Defines a list of networks to which traffic is sent in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.

- **Tunnel Network List Below**—Tunnels all traffic from or to the networks specified in the Network List. Traffic to addresses in the include network list are tunneled. Data to all other addresses travels in the clear and is routed by the remote user's Internet service provider.

  For versions of ASA 9.1.4 and higher, when you specify an include list, you can also specify an exclude list that is a subset of the include range. Those excluded subnets are not tunneled, and the rest of the include list networks are. Networks in the exclusion list that are not a subset of the include list are ignored by the client. For Linux, you must add a custom attribute to the group policy to support excluded subnets.

  For example:



Note
If the split-include network is an exact match of a local subnet (such as 192.168.1.0/24), the corresponding traffic is tunneled. If the split-include network is a superset of a local subnet (such as 192.168.0.0/16), the corresponding traffic, except the local subnet traffic, is tunneled. To also tunnel the local subnet traffic, you must add a matching split-include network (specifying both 192.168.1.0/24 and 192.168.0.0/16 as split-include networks).

If the split-include network is invalid, such as 0.0.0.0/0.0.0.0, then split tunneling is disabled (everything is tunneled).

- **Tunnel All Networks**—This policy specifies that all traffic is tunneled. This, in effect, disables split tunneling. Remote users reach Internet networks through the corporate network and do not have access to local networks. This is the default option.

Step 7 In the **Network List** field, choose the access control list for the split-tunneling policy. If Inherit is checked, the group policy uses the network list specified in the default group policy.

Select the **Manage** command button to open the ACL Manager dialog box, in which you can configure access control lists to use as network lists. For more information about how to create or edit a network list, see the general operations configuration guide.

Extended ACL lists can contain both IPv4 and IPv6 addresses.

Step 8 The **Intercept DHCP Configuration Message from Microsoft Clients** reveals additional parameters specific to DHCP Intercept. DHCP Intercept lets Microsoft XP clients use split-tunneling with the ASA.

- Intercept—Specifies whether to allow the DHCP Intercept to occur. If you do not choose Inherit, the default setting is No.
- Subnet Mask—Selects the subnet mask to use.

Step 9 Click **OK**.

Configure Dynamic Split Tunneling

With dynamic split tunneling, you can dynamically provision split exclude tunneling after tunnel establishment based on the host DNS domain name. Dynamic split tunneling is configured by creating a custom attribute and adding it to a group policy.

Before you begin

To use this feature, you must have AnyConnect release 4.5 (or later). Refer to About Dynamic Split Tunneling for further explanation.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-exclude-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 20,000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-exclude tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

What to do next

If split include tunneling is configured, a dynamic split exclusion is enforced only if at least one of the DNS response IP addresses is part of the split-include network. If there is no overlap between any of the DNS response IP addresses and any of the split-include networks, enforcing dynamic split exclusion is not necessary since traffic matching all DNS response IP addresses is already excluded from tunneling.

Configure Dynamic Split Exclude Tunneling

Follow these configuration steps to enable dynamic split exclude tunneling using ASDM. When both dynamic split exclude and include domains are defined, enhanced dynamic split exclude tunneling with domain name matching is enabled. For eample, an administrator could configure all traffic to example.com to be excluded except www.example.com. *Example.com* is the dynamic split exclude domain and *www.example.com* is the dynamic split include domain.

Note You must have AnyConnect release 4.5 (or later) to use dynamic split exclude tunneling. Additionally, AnyConnect release 4.6 (and later) added a refinement for enhanced dynamic split include and split exclude when domains for both are configured. Dynamic split exclude applies to all of tunnel-all, split-exclude and split-include configurations.

Before you begin

Refer to the *Dynamic Split Tunneling* section for AnyConnect Client requirements.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-exclude-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 5000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-exclude tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

Step 7 In the left-hand menu, click **Advanced >** AnyConnect Client **> Custom Attributes** and choose your attribute type from the drop down.

Configure Dynamic Split Include Tunneling

Follow these configuration steps to enable dynamic split include tunneling using ASDM. When both dynamic split exclude and include domains are defined, enhanced dynamic split include tunneling with domain name matching is enabled. For eample, an administrator could configure all traffic to domain.com to be included except www.domain.com. *Domain.com* is the dynamic split include domain and *www.domain.com* is the dynamic split exclude domain.

Note You must have AnyConnect release 4.6 (or later) to use dynamic split include tunneling. Additionally, AnyConnect release 4.6 (and later) added a refinement for enhanced dymanic split include and split exclude when domains for both are configured. Dynamic split include applies only to split-include configuration.

Before you begin

Refer to the *Dynamic Split Tunneling* section for AnyConnect Client requirements.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** screen.

Step 2 Click **Add** and enter `dynamic-split-include-domains` as an attribute type and enter a description.

Step 3 After you click to apply this new attribute, click on the **AnyConnect Client custom attribute names** link at the top of the UI screen.

Step 4 Add the corresponding custom attribute names for each cloud/web service that needs access by the client from outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. Define these domains in the Value portion of the AnyConnect Client Custom Attribute Names screen, using the comma-separated-values (CSV) format, which separates domains by a comma character. AnyConnect Client only takes into account the first 5000 characters, excluding separator characters (roughly 300 typically-sized domain names). Domain names beyond that limit are ignored.

A custom attribute cannot exceed 421 characters. If a larger value is entered, ASDM breaks it into multiple values capped at 421 characters. All values for a certain attribute type and name are concatenated by ASA when the configuration is pushed to the client.

Step 5 Attach the dynamic split-include tunneling attributes to a certain group policy by browsing to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 6 You can either create a new group policy or click **Edit** to manage an existing group policy.

Step 7 In the left-hand menu, click **Advanced >** AnyConnect Client **> Custom Attributes** and choose your attribute type from the drop down.

Configure the Management VPN Tunnel

A management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts which require corporate network connectivity will also benefit from this feature.

The management VPN tunnel is meant to be transparent to the end user; therefore, network traffic initiated by user applications is not impacted, by default, but instead directed outside the management VPN tunnel.

If a user complains of slow logins, it may be an indication that the management tunnel was not configured appropriately. Refer to the Cisco Secure Client Administration Guide for additional requirements, incompatibilities, limitations, and troubleshooting of management VPN tunnel.

Before you begin

Requires AnyConnect release 4.7 (or later)

Procedure

Step 1 You must configure the authentication method of the tunnel group as "certificate only" by navigating to **Configuration** > **Remote Access > Network (Client) Access >** AnyConnect Client **Connection Profiles > Add/Edit** and choosing it from the Method drop-down menu under Authentication.

Step 2 Then from that same window, choose **Advanced > Group Alias/Group URL** and add the group URL to be specified in the management VPN profile.

Step 3 The group policy for this tunnel group must have split include tunneling configured for all IP protocols with address pool configured in the the tunnel group: choose Tunnel Network List Below from **Remote Access VPN** > **Network (Client) Access > Group Policies > Edit > Advanced > Split Tunneling** .

Step 4 (Optional) Management VPN tunnel requires split include tunneling configuration, by default, to avoid impacting user initiated network communication (since it is meant to be transparent). You can override this behavior by configuring the custom attribute in the group policy used by the management tunnel connection: AnyConnect Client Custom Attributes, on page 143.
If an address pool is not configured in the tunnel group for both IP protocols, you must enable *Client Bypass Protocol* in the group policy, so that traffic matching the IP protocol without address pool is not disrupted by the management VPN tunnel.

Step 5 Create the profile and choose management VPN tunnel for profile usage: Configure AnyConnect Client Profiles, on page 128.

Configure Linux to Support Excluded Subnets

When **Tunnel Network List Below** is configured for split tunneling, Linux requires extra configuration to support exclude subnets. You must create a custom attribute named circumvent-host-filtering, set it to true, and associate with the group policy that is configured for split tunneling.

Procedure

Step 1 Connect to the ASDM, and navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Advanced** > AnyConnect Client **Custom Attributes.**

Step 2 Click **Add**, create a custom attribute named **circumvent-host-filtering**, and set the value to **true**.

Step 3 Edit the group policy you plan to use for client firewall, and navigate to **Advanced** > AnyConnect Client > **Custom Attributes**.

Step 4 Add the custom attribute that you created, **circumvent-host-filtering**, to the group policy you will use for split tunneling.

Internal Group Policy, AnyConnect Client Attributes

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced >AnyConnect Client, contains configurable attributes for the AnyConnect Client in this group policy.

- Keep Installer on Client System—Enable permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.



Note Keep Installer on Client System is not supported after version 2.5 of the AnyConnect Client.

- Datagram Transport Layer Security (DTLS)—Avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- DTLS Compression— Configures compression for DTLS.
- SSL Compression—Configures compression for SSL/TLS.
- Ignore Don't Defrag (DF) Bit—This feature allows the force fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel. An example use case is for servers in your network that do not respond correctly to TCP MSS negotiations.
- Client Bypass Protocol—Client Protocol Bypass configures how the AnyConnect Client manages IPv4 traffic when ASA is expecting only IPv6 traffic, or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

  When the AnyConnect Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. The Client Bypass Protocol determines whether to drop traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or "in the clear."

  For example, assume that the ASA assigns only an IPv4 address to an AnyConnect Client connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

- FQDN of This Device—This information is used by the client after network roaming in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support roaming between networks of different IP protocols (such as IPv4 to IPv6).



Note You cannot use the ASA FQDN present in the AnyConnect Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

If the device FQDN is not pushed to the client, the client tries to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name.

If the device FQDN is not pushed by the ASA, the client cannot re-establish the VPN session after roaming between networks of different IP protocols.

- MTU—Adjusts the MTU size for SSL connections. Enter a value in bytes, from 256 to 1410 bytes. By default, the MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.
- Keepalive Messages—Enter a number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that an connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.
- Optional Client Modules to Download—To minimize download time, the AnyConnect Client requests downloads (from the ASA) only of modules that it needs for each feature that it supports. You must specify the names of modules that enable other features. The AnyConnect Client, version 4.0, includes the following modules (previous versions have fewer modules):
  - AnyConnect Client DART—The Diagnostic AnyConnect Client Reporting Tool (DART) captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
  - AnyConnect Client Network Access Manager—Formerly called the Cisco Secure Services Client, this module provides 802.1X (Layer 2) and device authentication for access to both wired and wireless network.
  - AnyConnect Client SBL—Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect Client before the Windows login dialog box appears.
  - AnyConnect Client Web Security Module—Formerly called ScanSafe Hostscan, this module is integrated into AnyConnect Client. It deconstructs the elements of a web page so that it can analyze each element simultaneously. It can then allow acceptable content and block malicious or unacceptable content based on a security policy that is defined.
  - AnyConnect Client Telemetry Module—Sends information about the origin of malicious content to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.



Note Telemetry is not supported by AnyConnect 4.0.

  - ASA Posture Module—Formerly called the Cisco Secure Desktop HostScan feature, the posture module is integrated into AnyConnect Client and provides AnyConnect Client the ability to gather credentials for posture assessment prior to creating a remote access connection to the ASA.
  - ISE Posture—Uses the OPSWAT v3 library to perform posture checks to assess an endpoint's compliance. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges.
  - AMP Enabler—Used as medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base.

- Network Visibility Module—Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. The NVM collects the endpoint telemetry and logs both the flow data and the file reputation in the syslog and also exports the flow records to a collector (a third-party vendor), which performs the file analysis and provides a UI interface.
- Umbrella Roaming Security Module—Provides DNS-layer security when no VPN is active. It provides a subscription to either Cisco Umbrella Roaming service or OpenDNS Umbrella services, which add Intelligent Proxy and IP-Layer Enforcement features. The Umbrella Security Roaming profile associates each deployment with the corresponding service and automatically enables the corresponding protection level (whether content filtering, multiple policies, robust reporting, active directory integration, or basic DNS-layer security).

- Always-On VPN—Determine if the always-on VPN flag setting in the AnyConnect Client service profile is disabled or if the AnyConnect Client service profile setting should be used. The always-on VPN feature lets AnyConnnect automatically establish a VPN session after the user logs onto a computer. The VPN session remains up until the user logs off the computer. If the physical connection is lost, the session remains up, and AnyConnect Client continually attempts to reestablish the physical connection with the adaptive security appliance to resume the VPN session.

  Always-on VPN permits the enforcement of corporate policies to protect the device from security threats. You can use it to help ensure AnyConnect Client establishes a VPN session whenever the endpoint is not in a trusted network. If enabled, a policy is configured to determine how network connectivity is managed in the absence of a connection.



Note Always-On VPN requires an AnyConnect Client release that supports AnyConnect Secure Mobility features.

- Client Profiles to Download—A profile is a group of configuration parameters that the AnyConnect Client uses to configure VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, and Umbrella Roaming Security module settings. Click **Add** to launch the Select AnyConnect Client Profiles window, where you can specify previously created profiles for this group policy.

Internal Group Policy, AnyConnect Client Login Settings

In the Internal Group policy's **Advanced** > AnyConnect Client > **Login Setting** pane, you can enable the ASA to prompt remote users to download the AnyConnect Client, or direct the connection to a Clientless SSL VPN portal page.

- Post Login Setting—Choose to prompt the user and set the timeout to perform the default post login selection.
- Default Post Login Selection—Choose an action to perform after login.

Using Client Firewall to Enable Local Device Support for VPN

In the Internal Group policy's **Advanced** > **AnyConnect Client** > **Client Firewall** pane, you can configure rules to send down to the client system's firewall that affects how public and private networks are handled by the client.

When remote users connect to the ASA, all traffic is tunneled through the VPN connection, so users cannot access resources on their local network. This includes printers, cameras, and Windows Mobile devices (tethered devices) that synchronize with the local computer. Enabling Local LAN Access in the client profile resolves this problem, however it can introduce a security or policy concern for some enterprises as a result of unrestricted access to the local network. You can configure the ASA to deploy endpoint OS firewall rules that restrict access to particular types of local resources, such as printers and tethered devices.

To do so, enable client firewall rules for specific ports for printing. The client distinguishes between inbound and outbound rules. For printing capabilities, the client opens ports required for outbound connections, but blocks all incoming traffic.

Note Be aware that users logged in as administrators have the ability to modify the firewall rules deployed to the client by the ASA. Users with limited privileges cannot modify the rules. For either user, the client reapplies the firewall rules when the connection terminates.

If you configure the client firewall, and the user authenticates to an Active Directory (AD) server, the client still applies the firewall policies from the ASA. However, the rules defined in the AD group policy take precedence over the rules of the client firewall.

When client firewall rules are configured on the ASA, and the VPN connection is being established on the endpoint,

- The ASA sends the firewall rules information to the client.
- The client would then apply firewall rules as needed.

The following sections describe procedures on how to do this:

- Deploying a Client Firewall for Local Printer Support, on page 79
- Configure Tethered Devices Support for VPN, on page 81

Usage Notes about Firewall Behavior

The following notes clarify how the AnyConnect Client uses the firewall:

- The source IP is not used for firewall rules. The client ignores the source IP information in the firewall rules sent from the ASA. The client determines the source IP depending on whether the rules are public or private. Public rules are applied to all interfaces on the client. Private rules are applied to the Virtual Adapter.
- The ASA supports many protocols for ACL rules. However, the AnyConnect Client firewall feature supports only TCP, UDP, ICMP, and IP. If the client receives a rule with a different protocol, it treats it as an invalid firewall rule, and then disables split tunneling and uses full tunneling for security reasons.
- Starting in ASA 9.0, the Public Network Rule and Private Network Rule support unified access control lists. These access control lists can be used to define IPv4 and IPv6 traffic in the same rule.

Be aware of the following differences in behavior for each operating system:

- For Windows computers, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the AnyConnect Client, but the user has created a custom deny rule, the AnyConnect Client rule is not enforced.

- On Windows Vista, when a firewall rule is created, Vista takes the port number range as a comma-separated string. The port range can be a maximum of 300 ports. For example, from 1-300 or 5000-5300. If you specify a range greater than 300 ports, the firewall rule is applied only to the first 300 ports.
- Windows users whose firewall service must be started by the AnyConnect Client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.
- On Mac computers, the AnyConnect Client applies rules sequentially in the same order the ASA applies them. Global rules should always be last.
- For third-party firewalls, traffic is passed only if both the AnyConnect Client firewall and the third-party firewall allow that traffic type. If the third-party firewall blocks a specific traffic type that the AnyConnect Client allows, the client blocks the traffic.

Deploying a Client Firewall for Local Printer Support

The ASA supports the AnyConnect Client firewall feature with ASA version 8.3(1) or later, and ASDM version 6.3(1) or later. This section describes how to configure the client firewall to allow access to local printers, and how to configure the client profile to use the firewall when the VPN connection fails.

Limitations and Restrictions of the Client Firewall

The following limitations and restrictions apply to using the client firewall to restrict local LAN access:

- The *deny ip any any* private rules is not allowed.
- Due to limitations of the OS, the client firewall policy on computers running Windows XP is enforced for inbound traffic only. Outbound rules and bidirectional rules are ignored. This would include firewall rules such as 'permit ip any any'.
- HostScan (now named Secure Firewall Posture) and some third-party firewalls can interfere with the firewall.

The following table clarifies what direction of traffic is affected by the source and destination port settings:

Source Port	Destination Port	Traffic Direction Affected
Specific port number	Specific port number	Inbound and outbound
A range or 'All' (value of 0)	A range or 'All' (value of 0)	Inbound and outbound
Specific port number	A range or 'All' (value of 0)	Inbound only
A range or 'All' (value of 0)	Specific port number	Outbound only

Example ACL Rules for Local Printing

The ACL AnyConnect Client_Local_Print is provided with ASDM to make it easy to configure the client firewall. When you choose that ACL for Public Network Rule in the Client Firewall pane of a group policy, that list contains the following ACEs:

.

Table 3: ACL Rules in AnyConnect Client_Local_Print

Description	Permission	Interface	Protocol	Source Port	Destination Address	Destination Port
Deny all	Deny	Public	Any	Default	Any	Default
LPD	Allow	Public	TCP	Default	Any	515
IPP	Allow	Public	TCP	Default	Any	631
Printer	Allow	Public	TCP	Default	Any	9100
mDNS	Allow	Public	UDP	Default	224.0.0.251	5353
LLMNR	Allow	Public	UDP	Default	224.0.0.252	5355
NetBios	Allow	Public	TCP	Default	Any	137
NetBios	Allow	Public	UDP	Default	Any	137
Note The default port range is 1 to 65535.						

Note To enable local printing, you must enable the Local LAN Access feature in the client profile with a defined ACL rule allow Any Any.

Configure Local Print Support for VPN

To enable end users to print to their local printer, create a standard ACL in the group policy. The ASA sends that ACL to the VPN client, and the VPN client modify the client's firewall configuration.

Procedure

Step 1 Enable the AnyConnect Client firewall in a group policy. Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 2 Select a group policy and click **Edit**.

Step 3 Select **Advanced** > AnyConnect Client > **Client Firewall**. Click **Manage** for the Private Network Rule.

Step 4 Create an ACL containing the ACEs described above. Add this ACL as a Private Network Rule.

Step 5 If you enabled the Automatic VPN Policy always-on and specified a closed policy, in the event of a VPN failure, users have no access to local resources. You can apply the firewall rules in this scenario by going to **Preferences (Part 2)** in the profile editor and checking **Apply last local VPN resource rules**.

Configure Tethered Devices Support for VPN

To support tethered devices and protect the corporate network, create a standard ACL in the group policy, specifying destination addresses in the range that the tethered devices use. Then specify the ACL for split tunneling as a network list to exclude from tunneled VPN traffic. You must also configure the client profile to use the last VPN local resource rules in case of VPN failure.



Note For Windows Mobile devices that need to sync with the computer running AnyConnect Client, specify the IPv4 destination address as 169.254.0.0, or the IPv6 destination address fe80::/64 in the ACL.

Procedure

Step 1 In ASDM, go to **Group Policy > Advanced > Split Tunneling**.

Step 2 Uncheck **Inherit** next to the Network List field and click Manage.

Step 3 Click the **Extended ACL** tab.

Step 4 Click **Add > Add ACL**. Specify a name for the new ACL.

Step 5 Choose the new ACL in the table and click **Add** and then **Add ACE**.

Step 6 For **Action**, choose the **Permit radio** button.

Step 7 In the destination criteria area, specify the IPv4 destination address as 169.254.0.0 or the IPv6 destination address fe80::/64.

Step 8 For **Service**, choose IP.

Step 9 Click **OK**.

Step 10 Click **OK** to save the ACL.

Step 11 In the Split Tunneling pane for the internal group policy, uncheck Inherit for the Policy or IPv6 Policy, depending on the IP address you specified in step 7, and choose **Exclude Network List Below**. For Network List, choose the ACL you created.

Step 12 Click **OK**.

Step 13 Click **Apply**.

Internal Group Policy, AnyConnect Client Key Regeneration

Rekey Negotiation occurs when the ASA and the client perform a rekey and they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

In the Internal Group policy's **Advanced > AnyConnect Client > Key Regeneration** pane, you configure parameters for rekey:

- Renegotiation Interval—Uncheck the **Unlimited** check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- Renegotiation Method—Uncheck the Inherit check box to specify a renegotiation method different from the default group policy. Select the **None** radio button to disable rekey, choose either the **SSL** or **New Tunnel** radio button to establish a new tunnel during rekey.

Note Configuring the Renegotiation Method as **SSL** or **New Tunnel** specifies that the client establishes a new tunnel during rekey instead of the SSL renegotiation taking place during the rekey. See the command reference for a history of the **anyconnect ssl rekey** command.

Internal Group Policy, AnyConnect Client, Dead Peer Detection

Dead Peer Detection (DPD) ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed. To enable dead peer detection (DPD) and set the frequency with which either the AnyConnect Client or the ASA gateway performs DPD.

Note When the connection is interrupted on the client-side, ASA does not drop the AnyConnect Client sesssion because of DPD or keepalive unconditionally. DPD is only triggered by ASA when some data flow is there from ASA to client. Once DPD is triggered, it makes three retries for each child session (SSL/DTLS) before tearing them down.

If data flow is not there, DPD is not triggered, ASA has a hardcoded 5-minute TCP inactivity timeout that automatically closes SSL/DTLS tunnel connections when no data or keepalive packets flow for exactly 5 minutes, regardless of the configured VPN idle timeout setting. After the child sessions are teared down, **vpn-idle-timeout** command is only responsible for controlling the maximum time for a parent session. For further details on DPD, keepalives, and timeout attributes, see Answer AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer.

Before you begin

- This feature applies to connectivity between the ASA gateway and the AnyConnect Client SSL VPN Client only. It does not work with IPsec since DPD is based on the standards implementation that does not allow padding.
- If you enable DTLS, enable Dead Peer Detection (DPD) also. DPD enables a failed DTLS connection to fallback to TLS. Otherwise, the connection terminates.
- When DPD is enabled on the ASA, you can use the Optimal MTU (OMTU) function to find the largest endpoint MTU at which the client can successfully pass DTLS packets. Implement OMTU by sending a padded DPD packet to the maximum MTU. If a correct echo of the payload is received from the head end, the MTU size is accepted. Otherwise, the MTU is reduced, and the probe is sent again until the minimum MTU allowed for the protocol is reached.

Procedure

Step 1 Go to the desired group policy.

- Go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, **Add** or **Edit** the desired group policy, then open the **Advanced** > AnyConnect Client > **Dead Peer Detection** pane.

- Or, to reach a specific users policy, go to **Configuration > Device Management > Users/AAA > User Accounts**, Add or Edit the desired user account, then open the **VPN Policy >** AnyConnect Client **> Dead Peer Detection** pane.

Step 2 Set Gateway Side Detection.

Uncheck the **Disable** check box to specify that DPD is performed by the security appliance (gateway). Enter the interval, from 30 (default) to 3600 seconds, that the security appliance performs DPD. A value of 300 is recommended.

Step 3 Set Client Side Detection.

Uncheck the **Disable** check box to specify that DPD is performed by the client. Then enter the interval, from 30 (default) to 3600 seconds, that the client performs DPD. A value of 30 seconds is recommended.

Internal Group Policy, AnyConnect Client Customization of Clientless Portal

In the Internal Group policy's **Advanced > AnyConnect Client > Customization** pane, you can customize the Clientless Portal log on page for a group policy.

- Portal Customization—Selects the customization to apply to the AnyConnect Client/SSL VPN portal page. You can choose a preconfigured portal customization object, or accept the customization provided in the default group policy. The default is DfltCustomization.
  - Manage—Opens the Configure GUI Customization objects dialog box, in which you can specify that you want to add, edit, delete, import, or export a customization object.
- Homepage URL (optional)—Specifies a homepage URL to display in the Clientless Portal for users associated with the group policy. The string must begin with either http:// or https://. Clientless users are immediately brought to this page after successful authentication. AnyConnect Client launches the default web browser to this URL upon successful establishment of the VPN connection.

Note AnyConnect Client does not currently support this field on the Linux platform, Android mobile devices, and Apple iOS mobile devices. If set, it is ignored by these AnyConnect Clients.

- Use Smart Tunnel for Homepage—Create a smart tunnel to connect to the portal instead of using port forwarding.
- Access Deny Message—To create a message to display to users for whom access is denied, enter it in this field.

Configure AnyConnect Client Custom Attributes in an Internal Group Policy

The Internal Group policy's **Advanced > AnyConnect Client > Custom Attributes pane** lists the custom attributes that are currently assigned to this policy. In this dialog box you can associate previously defined custom attributes to this policy, or define custom attributes and then associate them with this policy.

Custom attributes are sent to and used by the AnyConnect Client to configure features such as Deferred Upgrade. A custom attribute has a type and a named value. The type of the attribute is defined first, then one

or more named values of this type can be defined. For details about the specific custom attributes to configure for a feature, see the *Cisco Secure Client Administrator Guide* for the AnyConnect Client release you are using.

Custom attributes can also be predefined in **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Client Custom Attributes** and **AnyConnect Client Custom Attribute Names**. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies.

Use this procedure to Add or Edit a custom attribute. You can also Delete a configured custom attribute, but custom attributes cannot be edited or deleted if they are also associated with another group policy.

Procedure

Step 1 Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **Advanced** > AnyConnect Client > **Custom Attributes**

Step 2 Click **Add** to open the **Create Custom Attribute** pane.

Step 3 Select a predefined **Attribute type** from the drop-down list or configure the attribute type by doing the following:

a) Click **Manage**, in the **Configure Custom Attribute Types** pane, click **Add**.

b) In the **Create Custom Attribute Type** pane, enter the new attribute **Type** and **Description**, both fields are required. For the AnyConnect Client custom attributes options, refer to AnyConnect Client Custom Attributes, on page 143.

c) Click **OK** to close this pane, then Click **OK** again to choose the newly defined custom attribute type.

Step 4 Choose **Select Value**.

Step 5 Select a predefined named value from the **Select value** drop-down list or configure a new named value by doing the following:

a) Click **Manage**, in the Configure Custom Attributes pane, click **Add**.

b) In the **Create Custom Attribute Name** pane, choose the attribute **Type** you previously selected or configured and enter the new attribute **Name** and **Value**, both fields are required.

To add a value, click **Add**, enter the value, and click **OK**. The value cannot exceed 420 characters. If your value exceeds this length, add multiple values for the additional value content. The configured values are concatenated before being sent to the AnyConnect Client.

c) Click **OK** to close this pane, then Click **OK** again to choose the newly defined named value of this attribute.

Step 6 Click **OK** in the **Create Custom Attribute** pane.

IPsec (IKEv1) Client Internal Group Policies

Internal Group Policy, General Attributes for IPsec (IKEv1) Client

The **Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client** Add or Edit Group Policy > IPsec dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified:

- Re-Authentication on IKE Re-key—Enables or disables reauthentication when IKE re-key occurs, unless the Inherit check box is checked. The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates.
- Allow entry of authentication credentials until SA expires—Allows users the time to reenter authentication credentials until the maximum lifetime of the configured SA.
- IP Compression—Enables or disables IP Compression, unless the Inherit check box is checked.
- Perfect Forward Secrecy—Enables or disables perfect forward secrecy (PFS), unless the Inherit check box is selected. PFS ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPsec protected data, and then use knowledge of the IKE SA secret to compromise the IPsec SAs set up by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPsec. The attacker would have to break each IPsec SA individually.
- Store Password on Client System—Enables or disables storing the password on the client system.



Note Storing the password on a client system can constitute a potential security risk.

- IPsec over UDP—Enables or disables using IPsec over UDP.
- IPsec over UDP Port—Specifies the UDP port to use for IPsec over UDP.
- Tunnel Group Lock—Locks the chosen tunnel group, unless the Inherit check box or the value None is selected.
- IPsec Backup Servers—Activates the Server Configuration and Server IP Addresses fields, so you can specify the UDP backup servers to use if these values are not inherited.
  - Server Configuration—Lists the server configuration options to use as an IPsec backup server. The available options are: Keep Client Configuration (the default), Use the Backup Servers Below, and Clear Client Configuration.
  - Server Addresses (space delimited)—Specifies the IP addresses of the IPsec backup servers. This field is available only when the value of the Server Configuration selection is Use the Backup Servers Below.

About Access Rules for IPsec (IKEv1) Client in an Internal Group Policy

The Client Access Rules table in this dialog box lets you view up to 25 client access rules. Configure the following fields when adding a client access rule:

- Priority—Select a priority for this rule.
- Action—Permit or deny access based on this rule.
- VPN Client Type—Specify the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset in free-form text.

- VPN Client Version—Specify the version or versions of the VPN client to which this rule applies. This column contains a comma-separated list of software or firmware images appropriate for this client. The entry is free-form text and ***** matches any version.

Client Access Rules Definitions

- If you do not define any rules, the ASA permits all connection types. But users might still inherit any rules that exist in the default group policy.
- When a client matches none of the rules, the ASA denies the connection. If you define a deny rule, you must also define at least one permit rule; otherwise, the ASA denies all connections.
- The * character is a wildcard, which you can enter multiple times in each rule.
- There is a limit of 255 characters for an entire set of rules.
- You can enter **n/a** for clients that do not send client type and/or version.

Internal Group Policy, Client Firewall for IPsec (IKEv1) Client

The Add or Edit Group Policy Client Firewall dialog box lets you configure firewall settings for VPN clients for the group policy being added or modified. Only VPN clients running on Microsoft Windows can use these firewall features. They are currently not available to hardware clients or other (non-Windows) software clients.

Remote users connecting to the ASA with the VPN client can choose the appropriate firewall option.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the ASA. (This firewall enforcement mechanism is called Are You There (AYT), because the VPN client monitors the firewall by sending it periodic “are you there?” messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the ASA.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called push policy or Central Protection Policy (CPP). On the ASA, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The ASA pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client > Client Firewall

Fields

- **Inherit**—Determines whether the group policy obtains its client firewall setting from the default group policy. This option is the default setting. When set, it overrides the remaining attributes in this dialog boxing dims their names.
- **Client Firewall Attributes**—Specifies the client firewall attributes, including what type of firewall (if any) is implemented and the firewall policy for that firewall.

- **Firewall Setting**—Lists whether a firewall exists, and if so, whether it is required or optional. If you choose No Firewall (the default), none of the remaining fields in this dialog box are active. If you want users in this group to be firewall-protected, choose either the Firewall Required or Firewall Optional setting.

  If you choose **Firewall Required**, all users in this group must use the designated firewall. The ASA drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the ASA notifies the VPN client that its firewall configuration does not match.



Note If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN clients. Any other clients in the group (including ASA 5505 in client mode) are unable to connect.

  If you have remote users in this group who do not yet have firewall capacity, choose **Firewall Optional**. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

- **Firewall Type**—Lists firewalls from several vendors, including Cisco. If you choose Custom Firewall, the fields under Custom Firewall become active. The firewall you designate must correlate with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported.
- **Custom Firewall**—Specifies the vendor ID, Product ID and description for the custom firewall.
  - **Vendor ID**—Specifies the vendor of the custom firewall for this group policy.
  - **Product ID**—Specifies the product or model name of the custom firewall being configured for this group policy.
  - **Description**—(Optional) Describes the custom firewall.
- **Firewall Policy**—Specifies the type and source for the custom firewall policy.
  - **Policy defined by remote firewall (AYT)**—Specifies that the firewall policy is defined by the remote firewall (Are You There). Policy defined by remote firewall (AYT) means that remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN client. The ASA allows VPN clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN client ends the session.
  - **Policy pushed (CPP)**—Specifies that the policy is pushed from the peer. If you choose this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active. The ASA enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down list. The choices available on the menu are filters defined in thisASA, including the default filters. Keep in mind that the ASA pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the ASA. For example, “in” and “out” refer to traffic coming into the VPN client or going outbound from the VPN client. If the VPN client also has a local firewall, the policy pushed from

the ASA works with the policy of the local firewall. Any packet that is blocked by the rules of either firewall is dropped.

- **Inbound Traffic Policy**—Lists the available push policies for inbound traffic.
- **Outbound Traffic Policy**—Lists the available push policies for outbound traffic.
- **Manage**—Displays the ACL Manager dialog box, in which you can configure Access Control Lists (ACLs).

Site-to-Site Internal Group Policies

The Group Policy for Site-to-Site VPN connections specifies tunneling protocols, filters, and connection settings. For each of the fields in this dialog box, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all of the attributes in this dialog box.

Fields

The following attributes appear in the Add Internal Group Policy > General dialog box. They apply to SSL VPN and IPsec sessions. Thus, several are present for one type of session, but not the other.

- Name—Specifies the name of this group policy. For the Edit function, this field is read-only.
- Tunneling Protocols—Specifies the tunneling protocols that this group allows. Users can use only the selected protocols. The choices are as follows:
  - Clientless SSL VPN—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to a ASA; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
  - SSL VPN Client—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client. If you are using the AnyConnect Client, you must choose this protocol for MUS to be supported.
  - IPsec IKEv1—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both Site-to-Site (peer-to-peer) connections and Cisco VPN client-to-LAN connections can use IPsec IKEv1.
  - IPsec IKEv2—Supported by the Secure Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
  - L2TP over IPsec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.
- **Filter**—(Network (Client) Access only) Specifies which access control list to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. Note that the VPN filter applies to initial connections only. It does not apply to secondary

connections, such as a SIP media connection, that are opened due to the action of application inspection. To configure filters and rules, see the Group Policy dialog box. Click **Manage** to open the ACL Manager, where you can view and configure ACLs.

- **Idle Timeout**—If the **Inherit** check box is not checked, this parameter sets the idle timeout in minutes.

  If there is no communication activity on the connection in this period, the system terminates the connection. The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.

- **Maximum Connect Time**—If the **Inherit** check box is not checked, this parameter sets the maximum user connection time in minutes.

  At the end of this time, the system terminates the connection. The minimum is 1minute, and the maximum is 35791394 minutes. To allow unlimited connection time, check **Unlimited** (default).

- **Periodic Certificate Authentication Interval**—The interval of time in hours, before certificate authentication is redone periodically.

  If the **Inherit** check box is not checked, you can set the interval for performing periodic certificate verification. The range is between 1 and 168 hours, and the default is disabled. To allow unlimited verification, check Unlimited.

Configure VPN Policy Attributes for a Local User

This procedure describes how to edit an existing user. To add a user choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users** and click **Add**. For more information see the general operations configuration guide.

Before you begin

By default the user account inherits the value of each setting from the default group policy, DfltGrpPolicy. To override each setting, uncheck the **Inherit** check box, and enter a new value.

Procedure

Step 1 Start ASDM and choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users**.

Step 2 Select the user you want configure and click **Edit**.

Step 3 In the left-hand pane, click **VPN Policy**.

Step 4 Specify a group policy for the user. The user policy will inherit the attributes of this group policy. If there are other fields on this screen that are set to **Inherit** the configuration from the Default Group Policy, the attributes specified in this group policy will take precedence over those set in the Default Group Policy.

Step 5 Specify which tunneling protocols are available for the user, or whether the value is inherited from the group policy.

Check the desired **Tunneling Protocols** check boxes to choose one of the following tunneling protocols:

- The SSL VPN Client lets users connect after downloading the AnyConnect Client application. Users use a clientless SSL VPN connection to download this application the first time. Client updates then occur automatically as needed whenever the user connects.

- IPsec IKEv1—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both Site-to-Site (peer-to-peer) connections and Cisco VPN client-to-LAN connections can use IPsec IKEv1.
- IPsec IKEv2—Supported by the AnyConnect Client. AnyConnect Client connections using IPsec with IKEv2 provide advanced features such as software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy.
- L2TP over IPsec allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the ASA and private corporate networks.

Note
If no protocol is selected, an error message appears.

Step 6 Specify which filter (IPv4 or IPv6) to use, or whether to inherit the value from the group policy.

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. Note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection.

a) To configure filters and rules, choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **General** > **More Options** > **Filter.**
b) Click **Manage** to display the ACL Manager pane, on which you can add, edit, and delete ACLs and ACEs.

Step 7 Specify whether to inherit the Connection Profile (tunnel group) lock or to use the selected tunnel group lock, if any.

Selecting a specific lock restricts users to remote access through this group only. Tunnel Group Lock restricts users by checking if the group configured in the VPN client is the same as the users assigned group. If it is not, the ASA prevents the user from connecting. If the Inherit check box is not checked, the default value is None.

Step 8 Specify whether to inherit the Store Password on Client System setting from the group.

Uncheck the **Inherit** check box to activate the Yes and No radio buttons. Click **Yes** to store the login password on the client system (potentially a less-secure option). Click **No** (the default) to require the user to enter the password with each connection. For maximum security, we recommend that you not allow password storage.

Step 9 Configure **Connection Settings**.

a) Specify an Access Hours policy to apply to this user, create a new access hours policy for the user, or leave the Inherit box checked. The default value is Inherit, or, if the Inherit check box is not checked, the default value is Unrestricted.

   Click **Manage** to open the Add Time Range dialog box, in which you can specify a new set of access hours.

b) Specify the number of simultaneous logins by the user. The Simultaneous Logins parameter specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.

   Note
   While there is no maximum limit, allowing several simultaneous connections could compromise security and affect performance.

c) Specify the **Maximum Connect Time** for the VPN connection in minutes. At the end of this time, the system terminates the connection.

If the **Inherit** check box is not checked, this parameter specifies the maximum user connection time in minutes. The minimum is 1minute, and the maximum is 35791394 minutes (over 4000 years). To allow unlimited connection time, check **Unlimited** (default).

d) Specify the **Idle Timeout** for the VPN connection in minutes. If there is no communication activity on the connection in this period, the system terminates the connection.

If the **Inherit** check box is not checked, this parameter specifies the idle timeout in minutes.The minimum time is 1 minute, the maximum time is 10080 minutes, and the default is 30 minutes. To allow unlimited connection time, check **Unlimited**.

Step 10 Configure **Timeout Alerts**.

a) Specify the **Maximum Connection Time Alert Interval**.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the max connection alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

b) Specify the **Idle Alert Interval**.

If you uncheck the **Inherit** check box, the **Default** check box is checked automatically. This sets the idle alert interval to 30 minutes. If you want to specify a new value, uncheck **Default** and specify a session alert interval from 1 to 30 minutes.

Step 11 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the **Dedicated IPv4 Address (Optional)** area.

Step 12 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the **Dedicated IPv6 Address (Optional)** area. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 13 Configure specific AnyConnect Client settings, by clicking on these options in the left-hand pane. To override each setting, uncheck the **Inherit** check box, and enter a new value.

Step 14 Click **OK** to apply the changes to the running configuration.

Connection Profiles

Connection Profiles, also known as tunnel-groups, configure connection attributes for VPN connections. These attributes apply to the AnyConnect VPN client, Clientless SSL VPN connections, and to IKEv1and IKEv2 third-party VPN clients.

AnyConnect Client Connection Profile, Main Pane

On the main pane of the AnyConnect Client Connection Profile you can enable client access on the interfaces, and add, edit, and delete connection profiles. You can also specify whether you want to allow a user to choose a particular connection at login.

- Access Interfaces—Lets you choose from a table the interfaces on which to enable access. The fields in this table include the interface name and check boxes specifying whether to allow access.

- In the Interface table, in the row for the interface you are configuring for AnyConnect Client connections, check the protocols you want to enable on the interface. You can allow SSL Access, IPsec access, or both.

  When checking SSL, DTLS (Datagram Transport Layer Security) is enabled by default. DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

  When checking IPsec (IKEv2) access, client services are enabled by default. Client services include enhanced AnyConnect Client features including software updates, client profiles, GUI localization (translation) and customization, Cisco Secure Desktop, and SCEP proxy. If you disable client services, the AnyConnect Client still establishes basic IPsec connections with IKEv2.

- Device Certificate—Lets you specify a certificate for authentication for either an RSA key or an ECDSA key. See Specify a Device Certificate, on page 93.
- Port Setting—Configure port numbers for HTTPS and DTLS (RA client only) connections. See Connection Profiles, Port Settings, on page 93.
- Bypass interface access lists for inbound VPN sessions—Enable inbound VPN sessions to bypass interface ACLs is checked by default. The security appliance allows all VPN traffic to pass through the interface ACLs. For example, even if the outside interface ACL does not permit the decrypted traffic to pass through, the security appliance trusts the remote private network and permits the decrypted packets to pass through. You can change this default behavior. If you want the interface ACL to inspect the VPN protected traffic, uncheck this box.

- Login Page Setting
  - Allow the user to choose a connection profile, identified by its alias, on the login page. If you do not check this check box, the default connection profile is DefaultWebVPNGroup.
  - Shutdown portal login page.—Shows the web page when the login is disabled.

- Connection Profiles—Configure protocol-specific attributes for connections (tunnel groups).
  - Add/Edit—Click to Add or Edit a Connection Profile (tunnel group).
  - Name—The name of the Connection Profile.
  - Aliases—Other names by which the Connection Profile is known.
  - SSL VPN Client Protocol—Specifies whether SSL VPN client have access.
  - Group Policy—Shows the default group policy for this Connection Profile.
  - Allow user to choose connection, identified by alias in the table above, at login page—Check to enable the display of Connection Profile (tunnel group) aliases on the Login page.

- Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.—This option specifies the relative preference of the group URL and certificate values during the connection profile selection process. If the ASA fails to match the preferred value, it chooses the connection profile that matches the other value. Check this option only if you want to rely on the preference used by many older ASA software releases to match the group URL specified by the VPN endpoint to the connection profile that specifies the same group URL. This option is unchecked by default. If it is unchecked, the ASA prefers to match

the certificate field value specified in the connection profile to the field value of the certificate used by the endpoint to assign the connection profile.

Specify a Device Certificate

The **Specify Device Certificate** pane allows you to specify a certificate that identifies the ASA to the client when it attempts to create a connection. This screen is for AnyConnect Client Connection Profiles and Clientless Connection Profiles. Certain AnyConnect Client features, such as Alway-on IPsec/IKEv2, require that a valid and trusted device certificate be available on the ASA.

As of ASA Release 9.4.1, ECDSA certificates can be used for SSL connections (from both AnyConnect Clients and Clientless SSL). Prior to this release, ECDSA certificates were only supported and configured for AnyConnect Client IPsec connections.

Procedure

Step 1 (For VPN connections only) In the **Certificate with RSA Key** area, perform one of these tasks:

- Keep the **Use the same device certificate for SSL and IPsec IKEv2** box checked if you want to choose one certificate to authenticate clients using either protocol. You can choose the certificate from those available in the list box or click **Manage** to create an identity certificate to use.
- Uncheck the **Use the same device certificate for SSL and IPsec IKEv2** check box to specify separate certificates for SSL connections or IPsec connections.

Step 2 Choose a certificate from the **Device Certificate** list box.

If you do not see the certificate you want, click the **Manage** button to manage the identity certificates on the ASA.

Step 3 (For VPN connections only) In the Certificate with ECDSA key field, choose the ECDSA certificate from the list box or click **Manage** to create an ECDSA identity certificate.

Step 4 Click **OK**.

Connection Profiles, Port Settings

Configure port numbers for SSL and DTLS connection (remote access only) connections in the connection profile panes in ASDM:

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Connection Profiles

Fields

- HTTPS Port—The port to enable for HTTPS (browser-based) SSL connections. The range is 1-65535. The default is port 443.
- DTLS Port—The UDP port to enable for DTLS connections. The range is 1-65535. The default is port 443.

AnyConnect Client Connection Profile, Basic Attributes

To set the basic attributes for an AnyConnect VPN module of Cisco Secure Client connection, choose Add or Edit in the AnyConnect Client Connection Profiles section. The Add (or Edit) AnyConnect Client Connection Profile > Basic dialog box opens.

- Name—For Add, specify the name of the connection profile you are adding. For Edit, this field is not editable.
- Aliases—(Optional) Enter one or more alternative names for the connection. You can add spaces or punctuation to separate the names.
- Authentication—Choose one of the following methods to use to authenticate the connection and specify a AAA server group to use in authentication.
  - Method— The authentication protocol has been extended to define a protocol exchange for multiple-certificate authentication and utilize this for both session types. You can validate multiple certificates per session with AnyConnect Client SSL and IKEv2 client protocols. Choose the type of authentication to use: AAA, AAA and certificate, Certificate only, SAML, Multiple certificates and AAA, Multiple certificates, SAML and certificate, or Multiple certificates and SAML. Depending on your selection, you may need to provide a certificate in order to connect.
  - AAA Server Group—Choose a AAA server group from the drop-down list. The default setting is LOCAL, which specifies that the ASA handles the authentication. Before making a selection, you can click **Manage** to open a dialog box over this dialog box to view or make changes to the ASA configuration of AAA server groups.
    - Choosing something other than LOCAL makes available the Use LOCAL if Server Group Fails check box.
    - Use LOCAL if Server Group fails—Check to enable the use of the LOCAL database if the group specified by the Authentication Server Group attribute fails.
- SAML Identity Provider—Choose the SAML IdP server for single sign-on (SSO) authentication.
  - SAML Server—Select the SAML server from the drop-down for AnyConnect Client single sign-on authentication, or click **Manage** to add an SSO server and configure the following parameters:
    - **IDP Entity ID**—The entity ID of the SAML Idp.
    - **Sign In URL**—URL for signing into the IdP. The url value must contain 4 to 500 characters.
    - **Sign Out URL**—(Optional) URL for redirecting to when signing out of the IdP. The url value must contain 4 to 500 characters.
    - **Base URL**—(Optional) URL is provided to third-party IdPs to redirect end-users back to the ASA.

      When base-url is configured, we use it as the base URL of the AssertionConsumerService and SingleLogoutService attribute in **show saml metadata**.

      When base-url is not configured, the URL is determined by the ASA's hostname and domain-name. For example, we use `https://ssl-vpn.cisco.com` when hostname is `ssl-vpn` and domain-name is `cisco.com`.

      An error occurs if neither base-url nor the hostname/domain-name are configured when entering **show saml metadata**.

- **Identity Provider Certificate**—Specifies the trustpoint that contains the IdP certificate for the ASA to verify SAML assertions. Choose a previously configured trustpoint.
- **Service Provider Certificate**—(Optional) Specifies the trustpoint that contains the ASA (SP)'s certificate for the IdP to verify ASA's signature or encrypted SAML assertion. Choose a previously configured trustpoint.
- **Request Signature**—Use the drop-down to choose which signing method you prefer for the SAML IdP server. You can choose rsa-sha1, rsa-sha256, rsa-sha384, or rsa-sha512.
- **Request Timeout**—(Optional) Timeout of the SAML request in seconds. The range is from 1 to 7200.

  If specified, this overrides NotOnOrAfter if the sum of NotBefore and timeout-in-seconds is earlier than NotOnOrAfter.

  If not specified, NotBefore and NotOnOrAfter in the assertion is used to determine the validity.
- **Enable IDP only accessible on internal network**—Check this check box to enable IDP only if it is accessible on the internal network.
- **Request IDP reauthentication at login**—Check this check box to enable IDP reauthentication at login.
- **Clock-skew**—Clock skew which will tolerate the NotBefore and NotOnOrAfter SAML assertions. By default, the clock-skew must be disabled. The default value is 1 second and the range is from 1 to 180 seconds.

- SAML IDP TrustPoint—Choose the SAML IdP TrustPoint for single sign-on (SSO) authentication.
  - IDP TrustPoint—Select the SAML IdP trustpoint that contains the IdP certificate for the ASA to verify SAML assertions.

- SAML Login Experience—Choose the SAML IdP TrustPoint for single sign-on (SSO) authentication.
  - VPN Client Embedded Browser—The VPN client uses its embedded browser for web authentication, so the authentication applies to the VPN connection only.
  - Default OS Browser—The VPN client uses the system’s default browser for web authentication. This option enables single sign-on (SSO) and support for web authentication methods, such as biometric authentication, that cannot be performed in the embedded browser.

    When you choose the default OS browser for SSO authentication, you must configure an external browser package for AnyConnect Client to use the default browser. See AnyConnect Client External Browser SAML Package, on page 126.

- SAML UserName Match—Select to match the certificate username to the SAML username.
- Client Address Assignment—Choose the DHCP servers, client address pools, and client IPv6 address pools to use.
- Client Address Assignment—Choose the DHCP servers, client address pools, and client IPv6 address pools to use.
  - DHCP Servers—Enter the name or IP address of a DHCP server to use.

- Client Address Pools—Enter pool name of an available, configured pool of IPv4 addresses to use for client address assignment. Before making a selection, you can click **Select** to open a dialog box over this dialog box to view or make changes to the address pools. See for more information on adding or editing an IPv4 address pool.
- Client IPv6 Address Pools—Enter the pool name of an available, configured pool of IPv6 addresses to use for client address assignment. Before making a selection, you can click **Select** to open a dialog box over this dialog box to view or make changes to the address pools. See for more information on adding or editing an IPv6 address pool.

•

- Default Group Policy—Select the group policy to use.
  - Group Policy—Select the VPN group policy that you want to assign as the default group policy for this connection. A VPN group policy is a collection of user-oriented attribute-value pairs that can be stored internally on the device or externally on a RADIUS server. The default value is DfltGrpPolicy. You can click **Manage** to open a dialog box over this one to make changes to the group policy configuration.
  - Enable SSL VPN client protocol—Check to enable SSL for this VPN connection.
  - Enable IPsec (IKEv2) client protocol—Check to enable IPsec using IKEv2 for this connection.
  - DNS Servers—Enter the IP address(s) of DNS servers for this policy.
  - WINS Servers—Enter the IP address(s) of WINS servers for this policy.
  - Domain Name—Enter a default domain name.
- Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Advanced Attributes

The Advanced menu items and their dialog boxes configure the following characteristics for this connection:

- General attributes
- Client Addressing attributes
- Authentication attributes
- Authorization attributes
- Accounting attributes
- Name server attributes



Note SSL VPN and secondary authentication attributes apply only to SSL VPN connection profiles.

AnyConnect Client Connection Profile, General Attributes

- Enable Simple Certificate Enrollment (SCEP) for this Connection Profile
- Strip the realm from username before passing it on to the AAA server
- Strip the group from username before passing it on to the AAA server
- Group Delimiter
- Enable Password Management—Lets you configure parameters relevant to notifying users about password expiration.
  - Notify user __ days prior to password expiration—Specifies that ASDM must notify the user at login a specific number of days before the password expires. The default is to notify the user 14 days prior to password expiration and every day thereafter until the user changes the password. The range is 1 through 180 days.
  - Notify user on the day password expires—Notifies the user only on the day that the password expires.

    In either case, and, if the password expires without being changed, the ASA offers the user the opportunity to change the password. If the current password has not expired, the user can still log in using that password.

    This does not change the number of days before the password expires, but rather, it enables the notification. If you choose this option, you must also specify the number of days.
- Translate Assigned IP Address to Public IP Address—In rare situations, you might want to use a VPN peer's real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer's real public IP address if, for example, your inside servers and network security is based on the peer's real IP address. You can enable this feature on one interface per tunnel group.
  - Enable the address translation on interface—Enables the address translation and allows you to choose which interface the address appears on. *Outside* is the interface to which the AnyConnect Client connects, and *inside* is the interface specific to the new tunnel group.



Note Because of routing issues and other limitations, we do not recommend using this feature unless you know you need it.

- Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Client Addressing

The Client Addressing pane on a connection profile assigns IP address pools on specific interfaces for use with this connection profile. The Client Addressing pane is common for all client connection profiles, and is available from the following ASDM paths:

- **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**

- **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles**
- **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv2) Connection Profiles**

The address pools you configure here can also be configured on the Basic pane of the Connection Profile.

The AnyConnect Client Connection Profile can assign IPv6 as well as IPv4 address pools.

To configure client addressing, open a remote access client connection profile (AnyConnect Client, IKEv1 or IKEv2), and select **Advanced** > **Client Addressing**.

- To view or change the configuration of address pools, click **Add** or **Edit** in the dialog box. The Assign Address Pools to Interface dialog box opens. This dialog box lets you assign IP address pools to the interfaces configured on the ASA. Click **Select**. Use this dialog box to view the configuration of address pools. You can change their address pool configuration as follows:
  - To add an address pool to the ASA, click **Add**. The Add IP Pool dialog box opens.
  - To change the configuration of an address pool on the ASA, click **Edit**. The Edit IP Pool dialog box opens if the addresses in the pool are not in use.

    You cannot modify an address pool if it is already in use. If you click **Edit** and the address pool is in use, ASDM displays an error message and lists the connection names and usernames that are using the addresses in the pool.
  - To remove address pool on the ASA, choose that entry in the table and click **Delete**.

    You cannot remove an address pool if it is already in use. If you click **Delete** and the address pool is in use, ASDM displays an error message and lists the connection names that are using the addresses in the pool.
- To assign address pools to an interface, click **Add**. The Assign Address Pools to Interface dialog box opens. Select the interface to be assigned an address pool. Click **Select** next to the Address Pools field. The Select Address Pools dialog box opens. Double-click each unassigned pool you want to assign to the interface or choose each unassigned pool and click **Assign**. The adjacent field displays the list of pool assignments. Click **OK** to populate the Address Pools field with the names of these address pools, then **OK** again to complete the configuration of the assignment.
- To change the address pools assigned to an interface, double-click the interface, or choose the interface and click **Edit**. The Assign Address Pools to Interface dialog box opens. To remove address pools, double-click each pool name and press the **Delete** button on the keyboard. Click **Select** next to the Address Pools field if you want to assign additional fields to the interface. The Select Address Pools dialog box opens. Note that the Assign field displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments. Click **OK** to revise the Address Pools field with the names of these address pools, then **OK** again to complete the configuration of the assignment.
- To remove an entry, choose the entry and click **Delete**.

Related Topics

Connection Profile, Client Addressing, Add or Edit, on page 99
Connection Profile, Address Pools, on page 99
Connection Profile, Advanced, Add or Edit IP Pool, on page 99

Connection Profile, Client Addressing, Add or Edit

To assign address pools to Connection Profile, select **Advanced > Client Addressing**, then select **Add** or **Edit**.

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, in which you can choose one or more address pools to assign to this interface. Your selection appears in the Address Pools field of the Assign Address Pools to Interface dialog box.

Connection Profile, Address Pools

The Select Address Pools dialog box in Connection Profile > Advanced shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment. You can add, edit, or delete connection profiles from that list.

- Add—Opens the Add IP Pool dialog box, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool dialog box, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments.

Connection Profile, Advanced, Add or Edit IP Pool

The Add or Edit IP Pool dialog box in Connection Profile > Advanced lets you specify or modify a range of IP addresses for client address assignment.

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

AnyConnect Client Connection Profile, Authentication Attributes

On the Connection Profile > Advanced >Authentication tab, you can configure the following fields:

- Interface-specific Authentication Server Groups—Manages the assignment of authentication server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.

- Username Mapping from Certificate—Lets you specify the methods and fields in a digital certificate from which to extract the username.



Note This feature is not supported in multiple context mode.

- Pre-fill Username from Certificate—Extracts the username from the specified certificate field and uses it for username/password authentication and authorization, according to the options that follow in this panel.
- Hide username from end user—Specifies to not display the extracted username to the end user.
- Use script to choose username—Specify the name of a script to use to choose a username from a digital certificate. The default is --None--.
- Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
- Delete—Deletes the selected script. There is no confirmation or undo.
- Use the entire DN as the username—Specifies that you want to use the entire Distinguished Name field of the certificate as the username.
- Specify the certificate fields to be used as the username—Specifies one or more fields to combine into the username.

  Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.

Attribute	Definition
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.

- Primary Field—Selects the first field to use from the certificate for the username. If this value is found, the secondary field is ignored.
- Secondary Field—Selects the field to use if the primary field is not found.

- Certificate Mapping for Multi-Certificate Authentication—Manages the assignment of certificate to be used for primary authentication.
  - First Certificate—Click this option if you want the machine issued certificate to be used for primary authentication.
  - Second Certificate—Click this option if you want the user certificate issued from client to be used for primary authentication.

- Find—Enter a GUI label or a CLI command to use as a search string, then click **Next** or **Previous** to begin the search.

Connection Profile, Secondary Authentication Attributes

Secondary Authentication under Connection Profile > Advanced lets you configure secondary authentication, which is also know as double authentication. When secondary authentication is enabled, the end user must present two sets of valid authentication credentials in order to log on. You can use secondary authentication in conjunction with pre-filling the username from a certificate. The fields in this dialog box are similar to those you configure for primary authentication, but these fields relate only to secondary authentication.

When double authentication is enabled, these attributes choose one or more fields in a certificate to use as the username. Configuring the secondary username from certificate attribute forces the security appliance to use the specified certificate field as the second username for the second username/password authentication.



Note If you also specify the secondary authentication server group, along with the secondary username from certificate, only the primary username is used for authentication.

- Secondary Authorization Server Group—Specifies an authorization server group from which to extract secondary credentials.
  - Server Group—Select an authorization server group to use as the secondary server AAA group. The default is none. The secondary server group cannot be an SDI server group.
  - Manage—Opens the Configure AAA Server Groups dialog box.

- Use LOCAL if Server Group fails—Specifies to fall back to the LOCAL database if the specified server group fails.
- Use primary username—Specifies that the login dialog must request only one username.
- Attributes Server—Select whether this is the primary or secondary attributes server.



Note If you also specify an authorization server for this connection profile, the authorization server settings take precedence—the ASA ignores this secondary authentication server.

- Session Username Server—Select whether this is the primary or secondary session username server.

- Interface-Specific Authorization Server Groups—Manages the assignment of authorization server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.
- Username Mapping from Certificate—Specify the fields in a digital certificate from which to extract the username.
- Pre-fill Username from Certificate—Check to extract the names to be used for secondary authentication from the primary and secondary fields specified in this panel. You must configure the authentication method for both AAA and certificates before checking this attribute. To do so, return to the Basic panel in the same window and check **Both** next to Method.
- Hide username from end user—Check to hide the username to be used for secondary authentication from the VPN user.
- Fallback when a certificate is unavailable —This attribute is configurable only if "Hide username from end user" is checked. Uses HostScan (now called Secure Firewall Posture) data to pre-fill the username for secondary authentication if a certificate is unavailable.
- Password—Choose one of the following methods to retrieve the password to be used for secondary authentication:
  - Prompt—Prompt the user for the password.
  - Use Primary—Reuse the primary authentication password for all secondary authentications.
  - Use—Enter a common secondary password for all secondary authentications.
- Specify the certificate fields to be used as the username—Specifies one or more fields to match as the username. To use this username in the pre-fill username from certificate feature for the secondary username/password authentication or authorization, you must also configure the pre-fill-username and secondary-pre-fill-username.
  - Primary Field—Selects the first field to use from the certificate for the username. If this value is found, the secondary field is ignored.

- Secondary Field—Selects the field to use if the primary field is not found.

The options for primary and secondary field attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.

- Use the entire DN as the username—Uses the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
- Use script to select username—Names the script from which to extract a username from a digital certificate. The default is --None--.
  - Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
  - Delete—Deletes the selected script. There is no confirmation or undo.
- Certificate Mapping for Multi-Certificate Authentication—Manages the assignment of certificate to be used for secondary authentication.

- First Certificate—Click this option if you want the machine issued certificate to be used for secondary authentication.
- Second Certificate—Click this option if you want the user certificate issued from client to be used for secondary authentication.

AnyConnect Client Connection Profile, Authorization Attributes

The Authorization dialog box in an AnyConnect Client Connection profile lets you view, add, edit, or delete interface-specific authorization server groups. Each row of the table in this dialog box shows the status of one interface-specific server group: the interface name, its associated server group, and whether fallback to the local database is enabled if the selected server group fails.

The fields in this pane are identical for AnyConnect Client, IKEv1, IKEv2 and Clientless SSL connection profiles.

- Authorization Server Group—Specifies an authorization server group from which to draw authorization parameters.
  - Server Group—Selects an authorization server group to use. The default is none.
  - Manage—Opens the Configure AAA Server Groups dialog box.
  - Users must exist in the authorization database to connect—Select this check box to require that users meet this criterion.
- Interface-specific Authorization Server Groups—Manages the assignment of authorization server groups to specific interfaces.
  - Add or Edit—Opens the Assign Authentication Server Group to Interface dialog box, in which you can specify the interface and server group, and specify whether to allow fallback to the LOCAL database if the selected server group fails. The Manage button in this dialog box opens the Configure AAA Server Groups dialog box. Your selections appear in the Interface/Server Group table.
  - Delete—Removes the selected server group from the table. There is no confirmation or undo.
- Username Mapping from Certificate—Specify the fields in a digital certificate from which to extract the username.
  - Use script to select username—Specifies the name of a script to use to choose a username from a digital certificate. The default is --None--. For more information about creating scripts to select create a username from certificate fields, see
  - Add or Edit—Opens the Add or Edit Script Content dialog box, in which you can define a script to use in mapping the username from the certificate.
  - Delete—Deletes the selected script. There is no confirmation or undo.
  - Use the entire DN as the username—Specifies that you want to use the entire Distinguished Name field of the certificate as the username.
  - Specify the certificate fields to be used as the username—Specifies one or more fields to combine into the username.

- Primary Field—Selects the first field to use in the certificate for the username. If this value is found, the secondary field is ignored.
- Secondary Field—Selects the field to use if the primary field is not found.

- Find—Enter a GUI label or a CLI command to use as a search string, then click Next or Previous to begin the search.

AnyConnect Client Connection Profile, Authorization, Add Script Content to Select Username

If you select **use a script to select username** in the Authorization pane of the AnyConnect Client, and you click the Add or Edit button, you will see the following fields.

Scripts can use certificate fields for authorization that are not listed in the other mapping options.



Note Both AnyConnect Client and clientless WebVPN display "Unknown" in the username field when pre-fill-username from certificate using a script cannot find the username in the client certificate.

- Script Name—Specify the name of the script. The script name must be the same in both authorization and authentication.You define the script here, and CLI uses the same script to perform this function.
- Select script parameters—Specify the attributes and content of the script.
- Value for Username—Select an attribute from the drop-down list of standard DN attributes to use as the username (Subject DN).
- No Filtering—Specify that you want to use the entire specified DN name.
- Filter by substring— Specify the Starting Index (the position in the string of the first character to match) and Ending Index (number of characters to search). If you choose this option, the starting index cannot be blank. If you leave the ending index blank, it defaults to -1, indicating that the entire string is searched for a match.

  For example, suppose you selected the DN attribute Common Name (CN), which contains a value of host/user. The following table shows some possible ways you might filter this value using the substring option to achieve various return values. The Return Value is what is actually pre-filled as the username.

Table 4: Filtering by Substring

Starting Index	Ending Index	Return Value
1	5	host/
6	10	user
6	-1	user

Using a negative index, as in the third row of this table, specifies to count from the end of the string backwards to the end of the substring, in this case, the "r" of "user."

When using filtering by substrings, you should know the length of the substring that you are seeking. From the following examples, use either the regular expression matching or the custom script in Lua format:

- Example 1: Regular Expression Matching—Enter a regular expression to apply to the search in the Regular Expression field. Standard regular expression operators apply. For example, suppose you want to use a regular expression to filter everything up to the @ symbol of the "Email Address (EA)" DN value. The regular expression ^[^@]* would be one way to do this. In this example, if the DN value contained a value of user1234@example.com, the return value after the regular expression would be user1234.
- Example 2: Use custom script in LUA format—Specify a custom script written in the LUA programming language to parse the search fields. Selecting this option makes available a field in which you can enter your custom LUA script; for example, the script:

```
return cert.subject.cn..'/'..cert.subject.l
```

combines two DN fields, username (cn) and locality (l), to use as a single username and inserts the slash (/) character between the two fields.

The table below lists the attribute names and descriptions that you can use in a LUA script.

Note LUA is case-sensitive.

Table 5: Attribute Names and Descriptions

Attribute Name	Description
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN qualifier
cert.subject.ea	E-mail Address
cert.subject.genq	Generational qualified
cert.subject.gn	Given Name
cert.subject.i	Initials
cert.subject.l	Locality
cert.subject.n	Name
cert.subject.o	Organization
cert.subject.ou	Organization Unit
cert.subject.ser	Subject Serial Number
cert.subject.sn	Surname
cert.subject.sp	State/Province
cert.subject.t	Title

cert.subject.uid	User ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN qualifier
cert.issuer.ea	E-mail Address
cert.issuer.genq	Generational qualified
cert.issuer.gn	Given Name
cert.issuer.i	Initials
cert.issuer.l	Locality
cert.issuer.n	Name
cert.issuer.o	Organization
cert.issuer.ou	Organization Unit
cert.issuer.ser	Issuer Serial Number
cert.issuer.sn	Surname
cert.issuer.sp	State/Province
cert.issuer.t	Title
cert.issuer.uid	User ID
cert.serialnumber	Certificate Serial Number
cert.subjectaltname.upn	User Principal Name

If an error occurs while activating a tunnel group script, causing the script not to activate, the administrator's console displays an error message.

Connection Profiles, Accounting

The Accounting pane in Connection Profile > Advanced sets accounting options globally across the ASA.

- Accounting Server Group—Choose the previously-defined server group to use for accounting.
- Manage—Opens the Configure AAA Server Groups dialog box, where you can create an AAA server group.

Connection Profile, Group Alias and Group URL

The GroupAlias/Group URL dialog box in Connection Profile > Advanced configures attributes that affect what the remote user sees upon login.

The name of the tab in the connection profile is Group URL/Group Alias for AnyConnect Client.

- **Login and Logout (Portal) Page Customization** (Clientless SSL VPN only)—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization. Click **Manage** to create a new customization object.
- **Enable the display of Radius Reject-Message on the login screen**—Select this check box to display the RADIUS-reject message on the login dialog box when authentication is rejected.
- **Enable the display of SecurId message on the login screen**—Select this check box to display SecurID messages on the login dialog box.
- **Connection Aliases**—The connection aliases and their status. A connection alias appears on the user login page if the connection is configured to allow users to choose a particular connection (tunnel group) at login. Click the buttons to **Add** or **Delete** aliases. To edit an alias, double-click the alias in the table and edit the entry. To change the enabled status, select or deselect the checkbox in the table.
- **Group URLs**—The group URLs and their status. A group URL appears on the user login page if the connection is configured to allow users to choose a particular group at login. Click the buttons to **Add** or **Delete** URLs. To **Edit** a URL, double-click the URL in the table and edit the entry. To change the enabled status, select or deselect the checkbox in the table.

IKEv1 Connection Profiles

IKEv1 connection profiles define authentication policies for native and third-party VPN clients, including L2TP-IPsec. IKEv1 connection profiles are configured on the **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles** pane.

- **Access Interfaces**—Selects the interfaces to enable for IPsec access. The default is no access.
- **Connection Profiles**—Shows in tabular format the configured parameters for existing IPsec connections. The Connections table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
  - **Name**—Specifies the name or IP address of the IPsec IKEv1 connection.
  - **IPsec Enabled**—Indicates whether the IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic dialog box.
  - **L2TP/IPsec Enabled**—Indicates whether the L2TP/IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic dialog box.
  - **Authentication Server Group**—Name of the group of servers that can provide authentication.
  - **Group Policy**—Indicates the name of the group policy for this IPsec connection.



Note Delete removes the selected server group from the table. There is no confirmation or undo.

IPsec Remote Access Connection Profile, Basic Tab

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box on **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Basic** lets you configure common attributes for IPsec IKEv1 VPN connections, including L2TP-IPsec.

- **Name**—Name of this connection profile.
- **IKE Peer Authentication**—Configures IKE peers.
  - **Pre-shared key**—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
  - **Identity Certificate**—Selects the name of an identity certificate, if any identity certificates are configured and enrolled. **Manage** opens the **Manage Identity Certificates** dialog box, on which you can add, edit, delete, export, and show details for a selected certificate.
- **User Authentication**—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.
  - **Server Group**—Selects the server group to use for user authentication. The default is LOCAL. If you select something other than LOCAL, the Fallback check box becomes available. To add a server group, click the **Manage** button.
  - **Fallback**—Specifies whether to use LOCAL for user authentication if the specified server group fails.
- **Client Address Assignment**—Specifies attributes relevant to assigning client attributes.
  - **DHCP Servers**—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
  - **Client Address Pools**—Specifies up to 6 predefined address pools. To define an address pool, click the **Select** button.
- **Default Group Policy**—Specifies attributes relevant to the default group policy.
  - **Group Policy**—Selects the default group policy to use for this connection. The default is DfltGrpPolicy. To define a new group policy to associate with this group policy, click **Manage**.
  - **Enable IPsec protocol** and **Enable L2TP over IPsec protocol**—Selects the protocol or protocols to use for this connection.

Add/Edit Remote Access Connections, Advanced, General

Use this dialog box to specify whether to strip the realm and group from the username before passing them to the AAA server, and to specify password management parameters.

- **Strip the realm from username before passing it on to the AAA server**—Enables or disables stripping the realm (administrative domain) from the username before passing the username on to the AAA server. Check the Strip Realm check box to remove the realm qualifier of the username during authentication. You can append the realm name to the username for AAA: authorization, authentication and accounting. The only valid delimiter for a realm is the @ character. The format is username@realm, for example, JaneDoe@example.com. If you check this Strip Realm check box, authentication is based on the username alone. Otherwise, authentication is based on the full username@realm string. You must check this box if your server is unable to parse delimiters.



Note You can append both the realm and the group to a username, in which case the ASA uses parameters configured for the group and for the realm for AAA functions. The format for this option is username[@realm]]<#or!>group], for example, JaneDoe@example.com#VPNGroup. If you choose this option, you must use either the # or ! character for the group delimiter because the ASA cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

The ASA does not include support for the user@grouppolicy. Only the L2TP/IPsec client supports the tunnel switching via user@tunnelgroup.

- **Strip the group from the username before passing it on to the AAA server**—Enables or disables stripping the group name from the username before passing the username on to the AAA server. Check Strip Group to remove the group name from the username during authentication. This option is meaningful only when you have also checked the Enable Group Lookup box. When you append a group name to a username using a delimiter, and enable Group Lookup, the ASA interprets all characters to the left of the delimiter as the username, and those to the right as the group name. Valid group delimiters are the @, #, and ! characters, with the @ character as the default for Group Lookup. You append the group to the username in the format username<delimiter>group, the possibilities being, for example, JaneDoe@VPNGroup, JaneDoe#VPNGroup, and JaneDoe!VPNGroup.
- **Password Management**—Lets you configure parameters relevant to overriding an account-disabled indication from a AAA server and to notifying users about password expiration.
  - **Enable notification upon password expiration to allow user to change password**—Checking this check box makes the following two parameters available. You can choose either to notify the user at login a specific number of days before the password expires or to notify the user only on the day that the password expires. The default is to notify the user 14 days prior to password expiration and every day thereafter until the user changes the password. The range is 1 through 180 days.



Note This does not change the number of days before the password expires, but rather, it enables the notification. If you choose this option, you must also specify the number of days.

In either case, and, if the password expires without being changed, the ASA offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This parameter is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

This feature requires the use of MS-CHAPv2.

IKEv1 Client Addressing

Client Addressing configuration is common for client Connection Profiles. See Connection Profile, Client Addressing, on page 97 for more information.

IKEv1 Connection Profile, Authentication

This dialog box is available for IPsec on Remote Access and Site-to-Site tunnel groups. The settings in this dialog box apply to this connection profile (tunnel group) globally across the ASA. To set authentication server group settings per interface, click **Advanced**. This dialog box lets you configure the following attributes:

- **Authentication Server Group**—Lists the available authentication server groups, including the LOCAL group (the default). You can also choose None. Selecting something other than None or Local makes available the Use LOCAL if Server Group Fails check box.
- **Use LOCAL if Server Group fails**—Enables or disables fallback to the LOCAL database if the group specified by the Authentication Server Group attribute fails.

  You can configure authentication on the basis of username alone by unchecking the Enable Group Lookup box. Checking both the Enable Group Lookup box and Strip Group lets you maintain a database of users with group names appended on your AAA server, and at the same time authenticate users on the basis of their username alone.

IKEv1 Connection Profile, Authorization

Configuring Authorization is common for client Connection Profiles. See AnyConnect Client Connection Profile, Authentication Attributes, on page 99 for more information.

IKEv1 Connection Profile, Accounting

Configuring Accounting is common for client Connection Profiles. See Connection Profiles, Accounting, on page 107 for more information.

IKEv1 Connection Profile, IPsec

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec

- **Send certificate chain**—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- **IKE Peer ID Validation**—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.

- **IKE Keep Alive**—Enables and configures ISAKMP keep alive monitoring.
  - **Disable Keep Alives**—Enables or disables ISAKMP keep alives.
  - **Monitor Keep Alives**—Enables or disables ISAKMP keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - **Confidence Interval**—Specifies the ISAKMP keep alive confidence interval. This is the number of seconds the ASA should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 300 seconds.
  - **Retry Interval**—Specifies number of seconds to wait between ISAKMP keep alive retries. The default is 2 seconds.
  - **Head end will never initiate keepalive monitoring**—Specifies that the central-site ASA never initiates keepalive monitoring.

IKEv1 Connection Profile, IPsec, IKE Authentication

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec > IKE Authentication

- **Default Mode**—Lets you choose the default authentication mode, none, xauth, or hybrid, as above.
- **Interface-Specific Mode**—Specifies the authentication mode on a per-interface basis.
  - **Add/Edit/Delete**—Add/Edit/Delete move an interface/authentication mode pair selection from the Interface/Authentication Modes table.
  - **Interface**—Select a named interface. The default interfaces are inside and outside, but if you have configured a different interface name, that name also appears in the list.
  - **Authentication Mode**—Lets you choose the authentication mode, none, xauth, or hybrid, as above.

IKEv1 Connection Profile, IPsec, Client Software Update

Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > IPsec > Client Software Update

Client VPN Software Update Table—Lists the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update dialog box) uses this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software.

- **Client Type**—Identifies the VPN client type.
- **VPN Client Revisions**—Specifies the acceptable revision level of the VPN client.
- **Location URL**—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For dialog boxes-based VPN clients, the URL must be of the form http:// or https://. For ASA 5505 in client mode, the URL must be of the form tftp://.

IKEv1 Connection Profile, PPP

To configure the authentication protocols permitted for a PPP connection using this IKEv1 Connection Profile, open **Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Advanced > PPP**.

This dialog box applies *only* to IPsec IKEv1 remote access connection profiles.

- **CHAP**—Enables the use of the CHAP protocol for a PPP connection.
- **MS-CHAP-V1**—Enables the use of the MS-CHAP-V1 protocol for a PPP connection.
- **MS-CHAP-V2**—Enables the use of the MS-CHAP-V2 protocol for a PPP connection.
- **PAP**—Enables the use of the PAP protocol for a PPP connection.
- **EAP-PROXY**—Enables the use of the EAP-PROXY protocol for a PPP connection. EAP refers to the Extensible Authentication protocol.

IKEv2 Connection Profiles

IKEv2 connection profiles define EAP, Certificate-based, and pre-shared key-based authentication for AnyConnect VPN module of Cisco Secure Clients. The configuration panel in ASDM is **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles**.

- Access Interfaces—Selects the interfaces to enable for IPsec access. The default is that no access is selected.
- Bypass interface access lists for inbound VPN sessions—Check this check box to bypass interface access lists for inbound VPN sessions. Access lists for group policy and user policy always apply to all traffic.
- Connection Profiles—Shows in tabular format the configured parameters for existing IPsec connections. The Connection Profiles table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
  - Name—Specifies the name or IP address of the IPsec connection.
  - IKEv2 Enabled—Specifies that the IKEv2 protocol is enabled if checked.
  - Authentication Server Group—Specifies the name of the server group used for authentication.
  - Group Policy—Indicates the name of the group policy for this IPsec connection.



Note Delete removes the selected server group from the table. There is no confirmation or undo.

IPsec IKEv2 Connection Profile, Basic Tab

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box configures common attributes for IPsec IKEv2 connections.

- **Name**—Identifies the name of the connection.
- **IKE Peer Authentication**—Configures IKE peers.
  - **Pre-shared key**—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
  - **Enable Certificate Authentication**—Allows you to use certificates for authentication if checked.
  - **Enable peer authentication using EAP**—Allows you to use EAP for authentication if checked. You must use certificates for local authentication if you check this check box.
  - **Send an EAP identity request to the client**—Enables you to send an EAP request for authentication to the remote access VPN client.
- Post Quantum Key—Check this check box to specify the post quantum pre-shared key (PPK). PPK is a 256-bit 64 character hexadecimal string and protects the session from quantum computer attacks.
  - Post Quantum Key Identity—Specify the ID of the PPK.
- **Mobike RRC**—Enable/disable mobike RRC.
  - **Enable Return Routability Check for mobike**—Enable/disable Return Routability checking for dynamic IP address changes in IKE/IPSEC security associations on which mobike is enabled.
- **User Authentication**—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.
  - **Server Group**—Selects the server group to use for user authentication. the default is LOCAL. If you choose something other than LOCAL, the Fallback check box becomes available.
  - **Manage**—Opens the Configure AAA Server Groups dialog box.
  - **Fallback**—Specifies whether to use LOCAL for user authentication if the specified server group fails.
- **Client Address Assignment**—Specifies attributes relevant to assigning client attributes.
  - **DHCP Servers**—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
  - **Client Address Pools**—Specifies up to 6 predefined address pools. Click Select to open the Address Pools dialog box.
- **Default Group Policy**—Specifies attributes relevant to the default group policy.
  - **Group Policy**—Selects the default group policy to use for this connection. The default is DfltGrpPolicy.
  - **Manage**—Opens the Configure Group Policies dialog box, from which you can add, edit, or delete group policies.

- **Client Protocols**—Selects the protocol or protocols to use for this connection. By default, both IPsec and L2TP over IPsec are selected.
- **Enable IKEv2 Protocol**—Enables the IKEv2 protocol for use in remote access connection profiles. This is an attribute of the group policy that you just selected.

IPsec Remote Access Connection Profile, Advanced, IPsec Tab

The IPsec table on IPsec (IKEv2) Connection Profiles has the following fields.

- Send certificate chain—Check to enable or disable sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- IKE Peer ID Validation—Choose from the drop-down list whether IKE peer ID validation is not checked, required, or checked if it is supported by a certificate.

Mapping Certificates to IPsec or SSL VPN Connection Profiles

When the ASA receives an IPsec connection request with client certificate authentication, it assigns a connection profile to the connection according to policies you configure. That policy can be to use rules you configure, use the certificate OU field, use the IKE identity (i.e. hostname, IP address, key ID), the peer IP address, or a default connection profile. For SSL connections, the ASA only uses the rules you configure.

For IPsec or SSL connections using rules, the ASA evaluates the attributes of the certificate against the rules until it finds a match. When it finds a match, it assigns the connection profile associated with the matched rule to the connection. If it fails to find a match, it assigns the default connection profile (DefaultRAGroup for IPsec and DefaultWEBVPNGroup for SSL VPN) to the connection and lets the user choose the connection profile from a drop-down list displayed on the portal page (if it is enabled). The outcome of the connection attempt once in this connection profile depends on whether or not the certificate is valid and the authentication settings of the connection profile.

A certificate group matching policy defines the method to use for identifying the permission groups of certificate users.

Configure the matching policy on the Policy pane. If you choose to use rules for matching, go to Rules pane to specify the rules.

Certificate to Connection Profile Maps, Policy

For IPsec connections, a certificate group matching policy defines the method to use for identifying the permission groups of certificate users. The settings for thse policies are configured on **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Policy**

- **Use the configured rules to match a certificate to a group**—Lets you use the rules you have defined under Rules.
- **Use the certificate OU field to determine the group**—Lets you use the organizational unit field to determine the group to which to match the certificate. This is selected by default.

- **Use the IKE identity to determine the group**—Lets you use the identity you previously defined under **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters**. The IKE identity can be hostname, IP address, key ID, or automatic.
- **Use the peer IP address to determine the group**—Lets you use the peer's IP address. This is selected by default.
- **Default to Connection Profile**—Lets you choose a default group for certificate users that is used when none of the preceding methods resulted in a match. This is selected by default. Click the default group in the Default to group list. The group must already exist in the configuration. If the group does not appear in the list, you must define it by using **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Certificate to Connection Profile Maps Rules

For IPsec connections, a certificate group matching policy defines the method to use for identifying the permission groups of certificate users. Profile maps are created on **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules**.

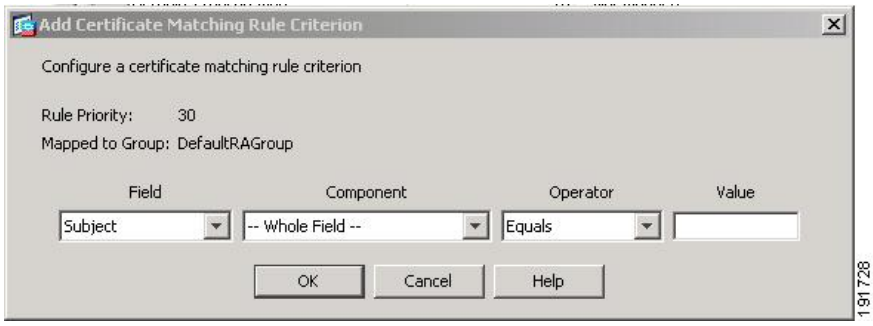
This pane has a list of certificate to connection profile maps, and mapping criteria.

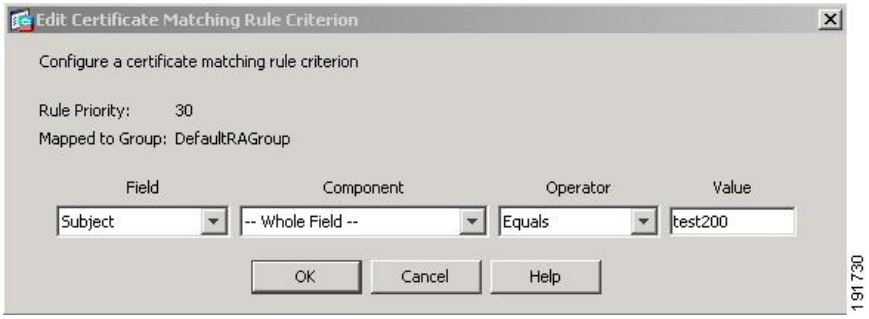
Certificate to Connection Profile Maps, add Certificate Matching Rule Criterion

Create map profiles to map connection profiles to mapping rules.

- Map—Choose one of the following:
  - Existing—Select the name of the map to include the rule.
  - New—Enter a new map name for a rule.
- Priority—Type a decimal to specify the sequence with which the ASA evaluates the map when it receives a connection request. For the first rule defined, the default priority is 10. The ASA evaluates each connection against the map with the lowest priority number first.
- Mapped to Connection Profile—Select the connection profile, formerly called a “tunnel group,” to map to this rule.

If you do not assign a rule criterion to the map, as described in the next section, the ASA ignores the map entry.





Add/Edit Certificate Matching Rule Criterion

Use this dialog box to configure a certificate matching rule criterion which you can map to a connection profile.

- Rule Priority—(Display only). Sequence with which the ASA evaluates the map when it receives a connection request. The ASA evaluates each connection against the map with the lowest priority number first.
- Mapped to Group—(Display only). Connection profile to which the rule is assigned.
- Field—Select the part of the certificate to be evaluated from the drop-down list.
  - Subject—The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
  - Alternative Subject—The subject alternative names extension allows additional identities to be bound to the subject of the certificate.
  - Issuer—The CA or other entity (jurisdiction) that issued the certificate.
  - Extended Key Usage—An extension of the client certificate that provides further criteria that you can choose to match.
- Component—(Applies only if Subject of Issuer is selected.) Select the distinguished name component used in the rule:

DN Field	Definition
Whole Field	The entire DN.
Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
DN Qualifier (DNQ)	A specific DN attribute.
E-mail Address (EA)	The e-mail address of the person, system or entity that owns the certificate.
Generational Qualifier (GENQ)	A generational qualifier such as Jr., Sr., or III.
Given Name (GN)	The first name of the certificate owner.

DN Field	Definition
Initials (I)	The first letters of each part of the certificate owner's name.
Locality (L)	The city or town where the organization is located.
Name (N)	The name of the certificate owner.
Organization (O)	The name of the company, institution, agency, association, or other entity.
Organizational Unit (OU)	The subgroup within the organization.
Serial Number (SER)	The serial number of the certificate.
Surname (SN)	The family name or last name of the certificate owner.
State/Province (S/P)	The state or province where the organization is located.
Title (T)	The title of the certificate owner, such as Dr.
User ID (UID)	The identification number of the certificate owner.
Unstructured Name (UNAME)	The unstructuredName attribute type specifies the name or names of a subject as an unstructured ASCII string.
IP Address (IP)	IP address field.

- Operator—Select the operator used in the rule:
  - Equals—The distinguished name field must exactly match the value.
  - Contains—The distinguished name field must include the value within it.
  - Does Not Equal—The distinguished name field must not match the value
  - Does Not Contain—The distinguished name field must not include the value within it.
- Value—Enter up to 255 characters to specify the object of the operator. For Extended Key Usage, choose one of the pre-defined values in the drop-down list, or you can enter OIDs for other extensions. The pre-defined values include the following:

Selection	Key Usage Purpose	OID String
clientauth	**Client Authentication**	**1.3.6.1.5.5.7.3.2**
codesigning	Code Signing	1.3.6.1.5.5.7.3.3
emailprotection	Secure Email Protection	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP Signing	1.3.6.1.5.5.7.3.9
serverauth	Server Authentication	1.3.6.1.5.5.7.3.1
timestamping	Time Stamping	1.3.6.1.5.5.7.3.8

Site-to-Site Connection Profiles

The Connection Profiles dialog box shows the attributes of the currently configured Site-to-Site connection profiles (tunnel groups), it also lets you choose the delimiter to use when parsing connection profile names, and lets you add, modify, or delete connection profiles.

The ASA supports IPsec LAN-to-LAN VPN connections for IPv4 or IPv6 using IKEv1 or IKEv2 and supports both inside and outside networks using the inner and outer IP headers.

Fields on the Site to Site Connection Profile Pane

- Access Interfaces—Displays a table of device interfaces where you can enable access by a remote peer device on the interface:
  - Interface—The device interface to enable or disable access.
  - Allow IKEv1 Access—Check to enable IPsec IKEv1 access by a peer device.
  - Allow IKEv2 Access—Check to enable IPsec IKEv2 access by a peer device.
- Connection Profiles—Displays a table of connection profiles where you can add, edit, or delete profiles:
  - Add—Opens the Add IPsec Site-to-Site connection profile dialog box.
  - Edit—Opens the Edit IPsec Site-to-Site connection profile dialog box.
  - Delete—Removes the selected connection profile. There is no confirmation or undo.
  - Name—The name of the connection profile.
  - Interface—The interface the connection profile is enabled on.
  - Local Network—Specifies the IP address of the local network.
  - Remote Network—Specifies the IP address of the remote network.
  - IKEv1 Enabled—Shows IKEv1 enabled for the connection profile.
  - IKEv2 Enabled—Shows IKEv2 enabled for the connection profile.
  - Group Policy—Shows the default group policy of the connection profile.

Add or Edit Site-to-Site Connection Profile

The Add or Edit IPsec Site-to-Site Connection dialog box lets you create or modify an IPsec Site-to-Site connection. These dialog boxes let you specify the peer IP address (IPv4 or IPv6), specify a connection name, choose an interface, specify IKEv1 and IKEv2 peer and user authentication parameters, specify protected networks, and specify encryption algorithms.



Note When you create a Site-to-Site VPN connection profile, open the connection profile and then cancel it without making any configuration changes, if you see the Apply button highlighted, discard the changes.

The ASA supports LAN-to-LAN VPN connections to Cisco or third-party peers when the two peers have IPv4 inside and outside networks (IPv4 addresses on the inside and outside interfaces).

For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the security appliance supports VPN tunnels if both peers are ASAs, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6).

Specifically, the following topologies are supported when both peers are ASAs:

- The ASAs have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces).
- The ASAs have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces).
- The ASAs have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces).

Fields on the Basic Panel

- Peer IP Address—Lets you specify an IP address (IPv4 or IPv6) and whether that address is static.
- Connection Name—Specifies the name assigned to this connection profile. For the Edit function, this field is display-only. You can specify that the connection name is the same as the IP address specified in the Peer IP Address field.
- Interface—Selects the interface to use for this connection.
- Protected Networks—Selects or specifies the local and remote network protected for this connection.
  - IP Address Type—Specifies the address is an IPv4 or IPv6 address.
  - Local Network—Specifies the IP address of the local network.
  - ...—Opens the Browse Local Network dialog box, in which you can choose a local network.
  - Remote Network—Specifies the IP address of the remote network.
- IPsec Enabling—Specifies the group policy for this connection profile and the key exchange protocol specified in that policy:
  - Group Policy Name—Specifies the group policy associated with this connection profile.
  - Manage—Opens the Browse Remote Network dialog box, in which you can choose a remote network.
  - Enable IKEv1—Enables the key exchange protocol IKEv1 in the specified group policy.
  - Enable IKEv2—Enables the key exchange protocol IKEv2 in the specified group policy.
- IKEv1 Settings tab—Specifies authentication and encryption settings for IKEv1:
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.

- Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
- IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
- Manage—Opens the Configure IKEv1 Proposals dialog box.
- IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.

- IKEv2 Settings tab—Specifies authentication and encryption settings for IKEv2:
  - Local Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Local Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.
  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - Remote Peer Pre-shared Key—Specify the value of the remote peer pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Remote Peer Certificate Authentication—Check Allowed to allow certificate authentication for IKEv2 connections for this connection profile.
  - Manage—Opens the Manage CA Certificates dialog where you can view certificates and add new ones.
  - Enable RSA Signature Hash—Check this check box to enable RSA signature hash. RSA is a type of encryption.
  - IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
  - Manage—Opens the Configure IKEv1 Proposals dialog box.
  - IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
  - Select—Opens the Select IPsec Proposals (Transform Sets) dialog box, where you can assign a proposal to the connection profile for IKEv2 connections.

This connection profile also has the following parameters:

- Advanced > Crypto Map Entry. For more information, see Site-to-Site Connection Profile, Crypto Map Entry, on page 123.

Site-to-Site Tunnel Groups

The ASDM pane **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups** specifies attributes for the IPsec site-to-site connection profiles (tunnel groups). In addition, you can choose IKE peer and user authentication parameters, configure IKE keepalive monitoring, and choose a default group policy.

- Name—Specifies the name assigned to this tunnel group. For the Edit function, this field is display-only.

- IKE Authentication—Specifies the pre-shared key and Identity certificate parameters to use when authenticating an IKE peer.
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Identity Certificate—Specifies the name of the ID certificate to use for authentication, if available.
  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - IKE Peer ID Validation—Specifies whether to check IKE peer ID validation. The default is Required.
- IPsec Enabling—Specifies the group policy for this connection profile and the key exchange protocol specified in that policy:
  - Group Policy Name—Specifies the group policy associated with this connection profile.
  - Manage—Opens the Browse Remote Network dialog box, in which you can choose a remote network.
  - Enable IKEv1—Enables the key exchange protocol IKEv1 in the specified group policy.
  - Enable IKEv2—Enables the key exchange protocol IKEv2 in the specified group policy.
- IKEv1 Settings tab—Specifies authentication and encryption settings for IKEv1:
  - Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
  - Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.



Note Some profiles may be unable to determine whether an endpoint is remote access or LAN-to-LAN. If it cannot determine the tunnel group, it defaults to

```
tunnel-group-map default-group <tunnel-group-name>
```

(default is *DefaultRAGroup*).

  - Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
  - IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
  - Manage—Opens the Configure IKEv1 Proposals dialog box.
  - IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
- IKEv2 Settings tab—Specifies authentication and encryption settings for IKEv2:
  - Local Pre-shared Key—Specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.

- Local Device Certificate—Specifies the name of the identity certificate, if available, to use for authentication.
- Manage—Opens the Manage Identity Certificates dialog box, on which you can see the certificates that are already configured, add new certificates, show details for a certificate, and edit or delete a certificate.
- Remote Peer Pre-shared Key—Specify the value of the remote peer pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
- Remote Peer Certificate Authentication—Check Allowed to allow certificate authentication for IKEv2 connections for this connection profile.
- Manage—Opens the Manage CA Certificates dialog where you can view certificates and add new ones.
- IKE Policy—Specifies one or more encryption algorithms to use for the IKE proposal.
- Manage—Opens the Configure IKEv1 Proposals dialog box.
- IPsec Proposal—Specifies one or more encryption algorithms to use for the IPsec IKEv1 proposal.
- Select—Opens the Select IPsec Proposals (Transform Sets) dialog box, where you can assign a proposal to the connection profile for IKEv2 connections.

- IKE Keepalive —Enables and configures IKE keepalive monitoring. You can choose only one of the following attributes.
  - Disable Keep Alives—Enables or disables IKE keep alives.
  - Monitor Keep Alives—Enables or disables IKE keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - Confidence Interval—Specifies the IKE keep alive confidence interval. This is the number of seconds the ASA should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 10 seconds.
  - Retry Interval—Specifies number of seconds to wait between IKE keep alive retries. The default is 2 seconds.
  - Head end will never initiate keepalive monitoring—Specifies that the central-site ASA never initiates keepalive monitoring.

Site-to-Site Connection Profile, Crypto Map Entry

In this dialog box, specify crypto parameters for the current Site-to-Site Connection Profile.

- **Priority**—A unique priority (1 through 65,543, with 1 the highest priority). When IKE negotiation begins, the peer that initiates the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order.
- **Perfect Forward Secrecy**—Ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). If someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If you enable PFS, the Diffie-Hellman Group list becomes active.

    - **Diffie-Hellman Group**—An identifier which the two IPsec peers use to derive a shared secret without transmitting it to each other. The choices are Group 1 (768-bits), Group 2 (1024-bits), and Group 5 (1536-bits).

- **Enable NAT-T**— Enables NAT Traversal (NAT-T) for this policy, which lets IPsec peers establish both remote access and LAN-to-LAN connections through a NAT device.
- **Enable Reverse Route Injection**—Provides the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint.
- **Security Association Lifetime**—Configures the duration of a Security Association (SA). This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys.
    - **Time**—Specifies the SA lifetime in terms of hours (hh), minutes (mm) and seconds (ss).
    - **Traffic Volume**—Defines the SA lifetime in terms of kilobytes of traffic. Enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.
- Static Crypto Map Entry Parameters—Configure these additional parameters when the Peer IP Address is specified as Static:
    - Connection Type—Specify the allowed negotiation as bidirectional, answer-only, or originate-only.
    - Send ID Cert. Chain—Enables transmission of the entire certificate chain.
    - IKE Negotiation Mode—Sets the mode for exchanging key information for setting up the SAs, Main or Aggressive. It also sets the mode that the initiator of the negotiation uses; the responder auto-negotiates. Aggressive Mode is faster, using fewer packets and fewer exchanges, but it does not protect the identity of the communicating parties. Main Mode is slower, using more packets and more exchanges, but it protects the identities of the communicating parties. This mode is more secure and it is the default selection. If you choose Aggressive, the Diffie-Hellman Group list becomes active.
    - Diffie-Hellman Group—An identifier which the two IPsec peers use to derive a shared secret without transmitting it to each other. The choices are Group 1 (768-bits), Group 2 (1024-bits), and Group 5 (1536-bits).

Managing CA Certificates

Managing CA Certificates applies to Remote Access and Site-to-Site VPN:

- On Site-to_site: Click Manage under IKE Peer Authentication to open the Manage CA Certificates dialog box.
- On Remote Access VPN, click **Certificate Management** > **CA Certificates**.

Use this dialog box to view, add, edit, and delete entries on the list of CA certificates available for IKE peer authentication. The Manage CA Certificates dialog box lists information about currently configured certificates, including information about whom the certificate was issued to, who issued the certificate, when the certificate expires, and usage data.

- Add or Edit—Opens the Install Certificate dialog box or the Edit Certificate dialog box, which let you specify information about and install a certificate.
- Show Details—Displays detailed information about a certificate that you choose in the table.
- Delete—Removes the selected certificate from the table. There is no confirmation or undo.

Site-to-Site Connection Profile, Install Certificate

Use this dialog box to install a new CA certificate. You can get the certificate in one of the following ways:

- Install from a file by browsing to the certificate file.
- Paste the previously acquired certificate text in PEM format into the box in this dialog box.
- Use SCEP—Specifies the use of the Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services runs on the Windows Server 2003 family. It provides support for the SCEP protocol, which allows Cisco routers and other intermediate network devices to obtain certificates.
  - SCEP URL: http://—Specifies the URL from which to download SCEP information.
  - Retry Period—Specifies the number of minutes that must elapse between SCEP queries.
  - Retry Count—Specifies the maximum number of retries allowed.
- More Options—Opens the Configure Options for CA Certificate dialog box.

Use this dialog box to specify details about retrieving CA Certificates for this IPsec remote access connection. The dialog boxes in this dialog box are: Revocation Check, CRL Retrieval Policy, CRL Retrieval Method, OCSP Rules, and Advanced.

Use the Revocation Check dialog box to specify information about CA Certificate revocation checking.

- The radio buttons specify whether to check certificates for revocation. Choose **Do not check certificates for revocation** or Check Certificates for revocation.
- Revocation Methods area—Lets you specify the method–CRL or OCSP–to use for revocation checking, and the order in which to use these methods. You can choose either or both methods.

AnyConnect VPN module of Cisco Secure Client Image

The **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software** pane lists the AnyConnect Client images that are configured in ASDM.

AnyConnect Client Images table—Displays the package files configured in ASDM, and allows you to establish the order that the ASA downloads the images to the remote PC.

- Add—Displays the Add AnyConnect Client Image dialog box, where you can specify a file in flash memory as a client image file, or you can browse flash memory for a file to specify as a client image. You can also upload a file from a local computer to the flash memory.
- Replace—Displays the Replace AnyConnect Client Image dialog box, where you can specify a file in flash memory as an client image to replace an image highlighted in the SSL VPN Client Images table. You can also upload a file from a local computer to the flash memory.

- Delete—Deletes an image from the table. This does not delete the package file from flash.
- Move Up and Move Down—The up and down arrows change the order in which the ASA downloads the client images to the remote PC. It downloads the image at the top of the table first. Therefore, you should move the image used by the most commonly-encountered operating system to the top.

AnyConnect VPN module of Cisco Secure Client Image, Add/Replace

In this pane, you can specify a filename for a file on the ASA flash memory that you want to add as an AnyConnect Client image, or to replace an image already listed in the table. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer.

- Flash SVC Image—Specify the file in flash memory that you want to identify as an SSL VPN client image.
- Browse Flash—Displays the Browse Flash dialog box where you can view all the files on flash memory.
- Upload—Displays the Upload Image dialog box where you can upload a file from a local PC that you want to identify as an client image.
- Regular expression to match user-agent—Specifies a string that the ASA uses to match against the User-Agent string passed by the browser. For mobile users, you can decrease the connection time of the mobile device by using the feature. When the browser connects to the ASA, it includes the User-Agent string in the HTTP header. When the ASA receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

AnyConnect VPN module of Cisco Secure Client Image, Upload Image

In this pane, you can specify the path of a file on the local computer or in flash memory of the security appliance that you want to identify as an AnyConnect Client image. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

- Local File Path—Identifies the filename of the file in on the local computer that you want to identify as an SSL VPN client image.
- Browse Local Files—Displays the Select File Path dialog box where you can view all the files on local computer and can choose a file to identify as a client image.
- Flash File System Path—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an SSL VPN client image.
- Browse Flash—Displays the Browse Flash Dialog dialog box where you can view all the files on flash memory of the security appliance and where you can choose a file to identify as a client image.
- Upload File—Initiates the file upload.

AnyConnect Client External Browser SAML Package

The **Configuration > Remote Access VPN > Network (Client) Access >AnyConnect External Browser** pane lists the AnyConnect Client external browser packages available for AnyConnect Client SAML single sign-on (SSO) authentication.

AnyConnect Client External Browser Package Images—Displays the external browser package files configured in ASDM.

- **Add**—Displays the Add AnyConnect Client External Browser Image dialog box, where you can specify a file in flash memory as an external package image file, or you can browse flash memory for a file to specify as the external browser package file.
- **Replace**—Displays the Replace AnyConnect Client External Browser Package dialog box, where you can specify a file in flash memory as an external browser package to replace an existing package file.
- **Delete**—Deletes an external browser package file from the table. This does not delete the package file from flash.
- **Move Up and Move Down**—The up and down arrows change the order in which the ASA downloads the external browser package to the remote PC.

AnyConnect Client External Browser SAML Package Images, Add/Replace

In this pane, you can specify a filename for a file on the ASA flash memory that you want to add as an AnyConnect Client external browser package image, or to replace an image already listed in the table. You can also browse the flash memory for a file to identify, or you can upload a file from a local computer.

- **AnyConnect Client External Browser Package** —Specify the file in flash memory that you want to identify as an external browser package image.
- **Browse Flash**—Displays the Browse Flash dialog box where you can view all the files on flash memory.
- **Upload**—Displays the Upload Image dialog box where you can upload a file from a local PC that you want to identify as an external browser package image.

AnyConnect Client External Browser SAML Package Images, Upload Image

In this pane, you can specify the path of a file on the local computer or in flash memory of the security appliance that you want to identify as an AnyConnect Client image. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

- **Local File Path**—Identifies the filename of the file in on the local computer that you want to identify as an external browser package image.
- **Browse Local Files**—Displays the Select File Path dialog box where you can view all the files on local computer and can choose a file to identify as an external browser package image..
- **Flash File System Path**—Identifies the filename of the file in the flash memory of the security appliance that you want to identify as an external browser package image.
- **Browse Flash**—Displays the Browse Flash Dialog dialog box where you can view all the files on flash memory of the security appliance and where you can choose a file to identify as an external browser package image..
- **Upload File**—Initiates the file upload.

Configure AnyConnect Client VPN Connections

Guidelines and Limitations for AnyConnect Client Connections

Recommendation for Session Tokens

When the ASA authenticates a VPN connection request from AnyConnect Client, a session token is returned to the client for enhanced security. Starting with AnyConnect 4.9 (MR1), the ASA and AnyConnect Client support a mechanism that provides enhanced security for the session token. You can configure a DAP rule to reject connection attempts from AnyConnect Client versions that do not support token security. See Use DAP to Check Session Token Security, on page 194.

Configure AnyConnect Client Profiles

You can configure the ASA to deploy AnyConnect Client profiles globally for all AnyConnect Client users or to users based on their group policy. Usually, a user has a single client profile for each AnyConnect Client module that is installed. In some cases, you might want to provide more than one profile for a user. Someone who works from multiple locations might need more than one profile. Be aware that some of the profile settings (such as SBL) control the connection experience at a global level. Other settings are unique to a particular host and depend on the host selected.

For more information about creating and deploying AnyConnect Client profiles and controlling client features, see the AnyConnect VPN Client Administrator Guide.

Client profiles are configured in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**:

Add/Import—Displays the Add AnyConnect Client Profiles dialog box, where you can specify a file in flash memory as a profile, or where you can browse flash memory for a file to specify as a profile. You can also upload a file from a local computer to the flash memory.

- Profile Name—Specify an AnyConnect Client profile for this group policy.
- Profile Usage—Displays the usage assigned to the profile when originally created: VPN, Network Access Manager, Web Security, ISE Posture, AMP Enabler, Network Visibility Module, Umbrella Roaming Security, or management VPN tunnel. If ASDM does not recognize the usage specified in the XML file, the drop-down list becomes selectable and you can choose a usage type manually.
- Profile Location—Specify a path to the profile file in the ASA flash memory. If the file does not exist, the ASA creates one based on the profile template.
- Group Policy—Specify a group policy for this profile. The profile downloads to users belonging to the group policy along with the AnyConnect Client.

Edit—Displays the Edit SSL VPN Client Profile window, where you can change the settings contained in the profile for AnyConnect Client features.

Export

- Device Profile Path—Displays the path and filename of the profile file.
- Local Path—Specify the path and filename to export the profile file.

- Browse Local—Click to launch a window to browse the local device file system.

Delete—Deletes a profile from the table. This does not delete the XML file from flash.

AnyConnect Client Profiles Table—Displays the XML files specified as AnyConnect Client profiles:

Exempt AnyConnect Client Traffic from Network Address Translation

If you have configured your ASA to perform network address translation (NAT), you must exempt your remote access the AnyConnect Client traffic from being translated so that the AnyConnect Clients, internal networks, and corporate resources on a DMZ, can originate network connections to each other. Failing to exempt the AnyConnect Client traffic from being translated prevents the AnyConnect Clients and other corporate resources from communicating.

"Identity NAT" (also known as "NAT exemption") allows an address to be translated to itself, which effectively bypasses NAT. Identity NAT can be applied between two address pools, an address pool and a subnetwork, or two subnetworks.

This procedure illustrates how you would configure identity NAT between these hypothetical network objects in our example network topology: Engineering VPN address pool, Sales VPN address pool, inside network, a DMZ network, and the Internet. Each Identity NAT configuration requires one NAT rule.

Table 6: Network Addressing for Configuring Identity NAT for VPN Clients

Network or Address Pool	Network or address pool name	Range of addresses
Inside network	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN address pool	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN address pool	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ network	DMZ-network	192.168.1.0 - 192.168.1.255

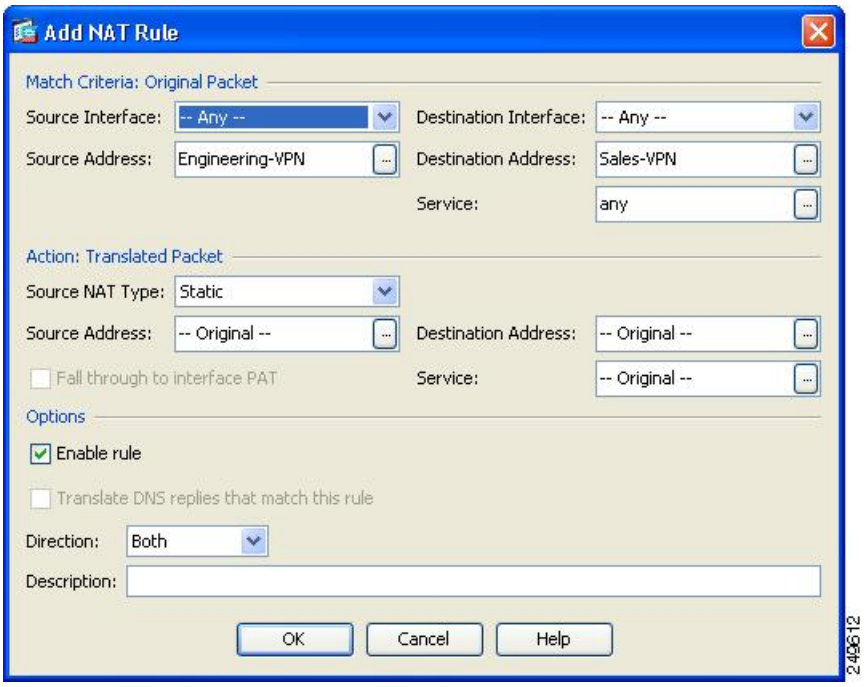
Procedure

Step 1 Log into the ASDM and navigate to **Configuration > Firewall > NAT Rules**.

Step 2 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach the hosts in the Sales VPN address pool. In the NAT Rules pane, navigate to **Add > Add NAT Rule** Before "Network Object" NAT rules so that the ASA evaluates this rule before other rules in the Unified NAT table.

Note
NAT rule evaluation is applied on a top-down, first match basis. Once the ASA matches a packet to a particular NAT rule, it does not perform any further evaluation. It is important that you place the most specific NAT rules at the top of the Unified NAT table so that the ASA does not prematurely match them to broader NAT rules.

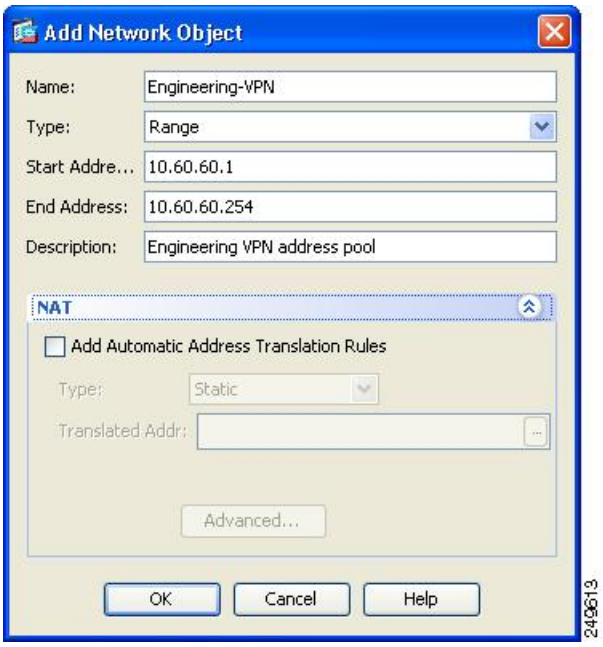
Figure 2: Add NAT rule dialog box



a) In the Match criteria: Original Packet area, configure these fields:

- **Source Interface**: Any
- **Destination Interface**: Any
- **Source Address**: Click the Source Address browse button and create the network object that represents the Engineering VPN address pool. Define the object type as a Range of addresses. Do not add an automatic address translation rule.
- **Destination Address**: Click the Destination Address browse button and create the network object that represents the Sales VPN address pool. Define the object type as a Range of addresses. Do not add an automatic address translation rule.

Figure 3: Create Network Object for a VPN address pool



b) In the **Action Translated Packet** area, configure these fields:

- **Source NAT Type**: Static
- **Source Address**: Original
- **Destination Address**: Original
- **Service**: Original

c) In the Options area, configure these fields:

- Check **Enable rule**.
- Uncheck or leave empty the **Translate DNS replies that match this rule**.
- **Direction**: Both
- **Description**: Add a Description for this rule.

d) Click **OK**.

e) Click **Apply**.

CLI example:

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN Sales-VPN
```

f) Click Send.

Step 3 When ASA is performing NAT, in order for two hosts in the same VPN pool to connect to each other, or for those hosts to reach the Internet through the VPN tunnel, you must enable the Enable traffic between two or more hosts connected to the same interface option. To do this, in ASDM, choose **Configuration > Device**

Setup > Interface Settings > Interfaces. At the bottom of the Interface panel, check Enable traffic between two or more hosts connected to the same interface and click Apply.

CLI example:

```
same-security-traffic permit inter-interface
```

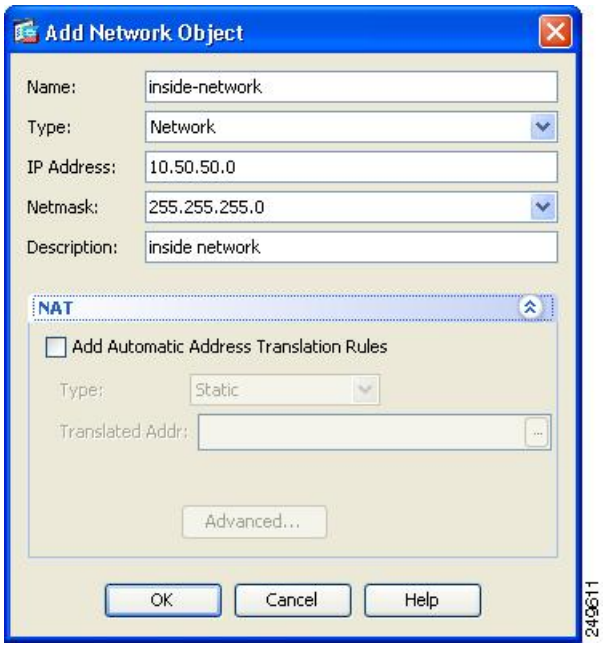
Step 4 Create a NAT rule so that the hosts in the Engineering VPN address pool can reach other hosts in the Engineering VPN address pool. Create this rule just as you created the rule in in the previously, except that you specify the Engineering VPN address pool as both the Source address and the Destination Address in the Match criteria: Original Packet area.

Step 5 Create a NAT rule so that the Engineering VPN remote access clients can reach the "inside" network. In the NAT Rules pane, choose Add > Add NAT Rule Before "Network Object" NAT rules so that this rule will be processed before other rules.

a) In the Match criteria: Original Packet area configure these fields:

- Source Interface: Any
- Destination Interface: Any
- Source Address: Click the Source Address browse button and create a network object that represents the inside network. Define the object type as a Network of addresses. Do not add an automatic address translation rule.
- Destination Address: Click the Destination Address browse button and choose the network object that represents the Engineering VPN address pool.

Figure 4: Add inside-network object



b) In the Action: Translated Packet area, configure these fields:

- Source NAT Type: Static

- Source Address: Original
- Destination Address: Original
- Service: Original

c) In the **Options** area, configure these fields:

- Check **Enable rule**.
- Uncheck or leave empty the **Translate DNS replies that match this rule**.
- Direction: Both
- Description: Add a Description for this rule.

d) Click **OK**.

e) Click **Apply**.

CLI example

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

Step 6 Create a new rule, following the method in **Step 5**, to configure identity NAT for the connection between the Engineering VPN address pool and the DMZ network. Use the DMZ network as the Source Address and use the Engineering VPN address pool as the Destination address.

Step 7 Create a new NAT rule to allow the Engineering VPN address pool to access the Internet through the tunnel. In this case, you do not want to use identity NAT because you want to change the source address from a private address to an Internet routable address. To create this rule, follow this procedure:

a) In the NAT Rules pane, choose Add > Add NAT Rule Before "Network Object" NAT rules so that this rule will be processed before other rules.

b) In the Match criteria: Original Packet area configure these fields:

- Source Interface: Any
- Destination Interface: Any. This field will be automatically populated with "outside" after you choose outside as the Source Address in the Action: Translated Packet area.
- Source Address: Click the Source Address browse button and choose the network object that represents the Engineering VPN address pool.
- Destination Address: Any.

c) In the Action: Translated Packet area, configure these fields:

- Source NAT Type: Dynamic PAT (Hide)
- Source Address: Click the Source Address browse button and choose the outside interface.
- Destination Address: Original
- Service: Original

d) In the Options area, configure these fields:

- Check Enable rule.

- Uncheck or leave empty the Translate DNS replies that match this rule.
- Direction: Both
- Description: Add a Description for this rule.

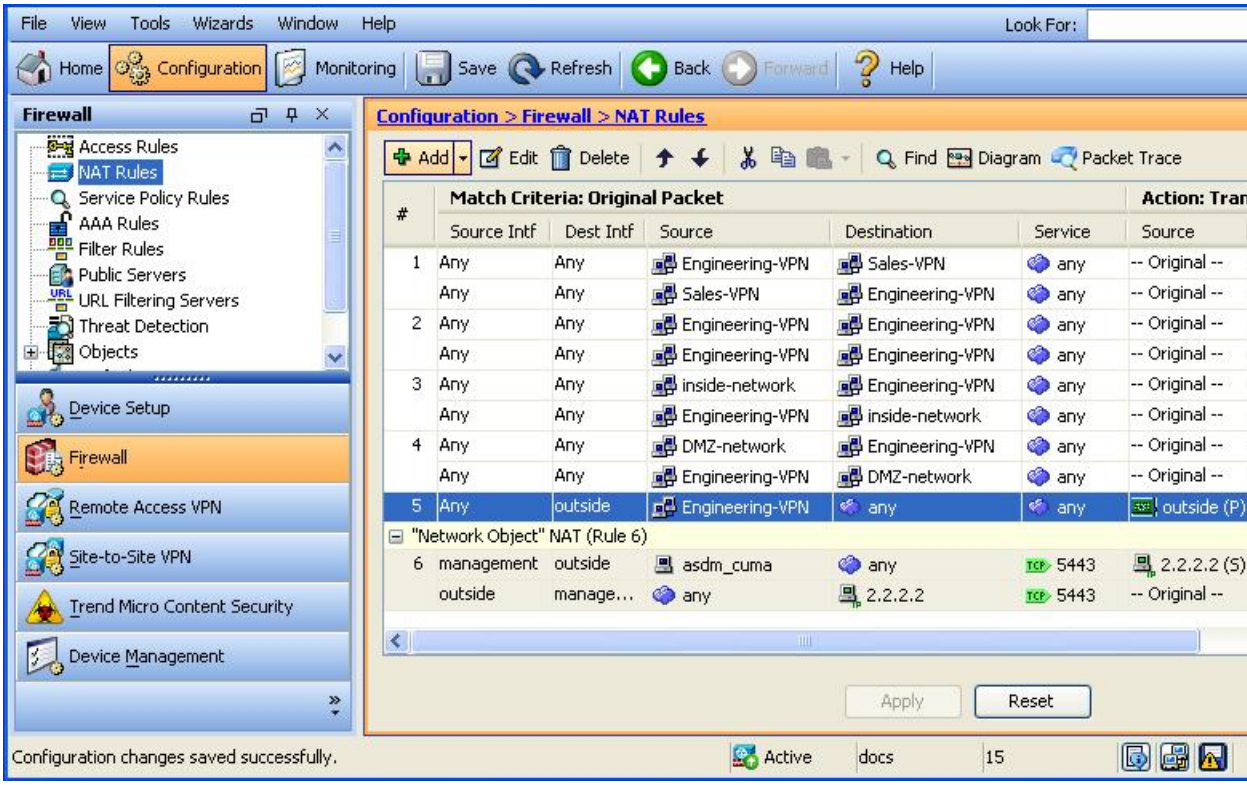
e) Click **OK**.

f) Click **Apply**.

CLI example:

```
nat (any,outside) source dynamic Engineering-VPN interface
```

Figure 5: Unified NAT table



Step 8 After you have configured the Engineering VPN Address pool to reach itself, the Sales VPN address pool, the inside network, the DMZ network, and the Internet; you must repeat this process for the Sales VPN address pool. Use identity NAT to exempt the Sales VPN address pool traffic from undergoing network address translation between itself, the inside network, the DMZ network, and the Internet.

Step 9 From the **File** menu on the ASA, choose **Save Running Configuration to Flash** to implement your identity NAT rules.

AnyConnect Client HostScan

AnyConnect Client HostScan, now called Secure Firewall Posture, provides the Secure Client the ability to identify the operating system, antimalware, and firewall software installed on the host. The Secure Firewall Posture/HostScan application gathers this information. Posture assessment requires Secure Firewall Posture/HostScan to be installed on the host.

The ASDM UI is dynamic in that if HostScan is loaded, it will reflect HostScan. When Secure Firewall Posture is loaded, it will reflect Secure Firewall Posture. The different naming depends on the version you are running.

Prerequisites for HostScan/Secure Firewall Posture

The AnyConnect Client with the Secure Firewall Posture/HostScan module requires these minimum ASA components:

- ASA 8.4
- ASDM 6.4

You must install Secure Firewall Posture/HostScan to use the SCEP authentication feature.

Refer to Supported VPN Platforms, Cisco ASA Series for what operating systems are supported for Secure Firewall Posture/HostScan installation.

Licensing for AnyConnect Client HostScan/Secure Firewall Posture

These are the licensing requirements for Secure Firewall Posture/HostScan:

- AnyConnect Client Advantage (Apex) for basic HostScan/Secure Firewall Posture.
- Advanced Endpoint Assessment license is required for remediation.

HostScan Packaging

You can load the HostScan package on to the ASA as a standalone package: **hostscan-version.pkg**. This file contains the HostScan software as well as the HostScan library and support charts.

Install or Upgrade HostScan/Secure Firewall Posture

Use this procedure to install or upgrade the HostScan/Secure Firewall Posture package and enable it using ASDM. The ASDM UI is dynamic in that if HostScan is loaded, it will reflect HostScan. When Secure Firewall Posture is loaded, it will reflect Secure Firewall Posture. The different naming depends on the version you are running.

Before you begin

Note If you are attempting to upgrade to HostScan version 4.6.x or later from a 4.3.x version or earlier, you will receive an error message due to the fact that all existing AV/AS/FW DAP policies and LUA script(s) that you have previously established are incompatible with HostScan 4.6.x or greater.

There is a one time migration procedure that must be done to adapt your configuration. This procedure involves leaving this dialog box to migrate your configuration to be comptaible with HostScan 4.4.x before saving this configuration. Abort this procedure and refer to the AnyConnect Client HostScan 4.3.x to 4.6.x Migration Guide for detailed instructions. Briefly, migration involves navigating to the ASDM DAP policy page to review and manually deleting the incompatible AV/AS/FW attributes, and then reviewing and rewriting LUA scripts.

Procedure

Step 1 Download the secure-firewall-posture-*version*-k9.pkg file to your computer if you are using version 5. For version 4.x, the file is hostscan_*version*-k9.pkg.

Step 2 Open ASDM and choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Image**. If you are using the HostScan 4.x version, the path will be **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

Step 3 Click **Upload** to prepare to transfer a copy of the HostScan/Secure Firewall Posture package from your computer to a drive on the ASA.

Step 4 In the Upload Image dialog box, click **Browse Local Files** to search for the HostScan/Secure Firewall Posture package on your local computer.

Step 5 Choose the hostscan_*version*-k9.pkg or secure-firewall-posture-*version*-k9.pkg file you downloaded above and click **Select**. The path to the file you selected is in the Local File Path field, and the Flash File System Path field reflects the destination path of the HostScan/Secure Firewall Posture package. If your ASA has more than one flash drive, you can edit the Flash File System Path to indicate another flash drive.

Step 6 Click **Upload File.** ASDM transfers a copy of the file to the flash card. An Information dialog box displays that the file has been successfully uploaded to flash.

Step 7 Click **OK**.

Step 8 In the Use Uploaded Image dialog, click **OK** to use the HostScan/Secure Firewall Posture package file you just uploaded as the current image.

Step 9 Check **Enable HostScan** or **Enable Posture Image**if it is not already checked.

Step 10 Click **Apply**.

Step 11 From the File menu, choose **Save Running Configuration To Flash**.

Configure Posture Settings

For each device, you can configure the posture settings.

Before you begin

Ensure that you have the HostScan/Secure Firewall Posture package.

Procedure

Step 1 Choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings**.

Step 2 In the left pane, select a device from the device list.

For each device, you can view the **Basic Posture** attributes and the **Posture Extensions**.

Step 3 By default, the Endpoint Detection and Response (EDR) security software communicates with its respective server to retrieve information. You can configure the following settings for EDR updates:

- Check the **For EDR update, Skip Internet Check after VPN is active** check box if you want the EDR to skip the internet connection check when the VPN tunnel is active.
- Check the **For EDR update, Skip Internet Check before VPN is active** check box to enable HostScan/Secure Firewall Posture assessment without verifying if the security software is up-to-date. If you uncheck the check box, the posture assessment may fail due to lack of connectivity, resulting in denied network access depending on the policy. We recommend that you verify the internet connectivity before posture assessment.

Uninstall HostScan/Secure Firewall Posture

Uninstalling HostScan/Secure Firewall Posture package removes it from view on the ASDM interface and prevents the ASA from deploying it even when it is enabled. Uninstalling HostScan/Secure Firewall Posture does not delete the package from the flash drive.

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Image** to uninstall Secure Firewall Posture. If you are using AnyConnect version 4.x and uninstalling HostScan, navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

Step 2 Click **Uninstall**, and then **Yes** to confirm.

Step 3 Click **Uninstall**.

Assign AnyConnect Client Feature Modules to Group Policies

This procedure associates AnyConnect Client feature modules with a group policy. When VPN users connect to the ASA, the ASA downloads and installs these AnyConnect Client feature modules to their endpoint computer.

Before you begin

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: hostname(config)#

Procedure

Step 1 Adds an internal group policy for Network Client Access

group-policy *name* **internal**

Example:

```
hostname(config)# group-policy PostureModuleGroup internal
```

Step 2 Edit the new group policy. After entering the command, you receive the prompt for group policy configuration mode, hostname(config-group-policy)#.

group-policy *name* **attributes**

Example:

```
hostname(config)# group-policy PostureModuleGroup attributes
```

Step 3 Enter group policy webvpn configuration mode. After you enter the command, the ASA returns this prompt: hostname(config-group-webvpn)#

webvpn

Step 4 Configure the group policy to download the AnyConnect Client feature modules for all users in the group.

anyconnect modules value *AnyConnect Module Name*

The value of the anyconnect module command can contain one or more of the following values. When specifying more than one module, separate the values with a comma:

value	AnyConnect Module/Feature Name
dart	AnyConnect DART (Diagnostics and Reporting Tool)
vpngina	AnyConnect SBL (Start Before Logon)
posture	Secure Firewall Posture/HostScan
nam	AnyConnect Network Access Manager
none	Used by itself to remove all AnyConnect modules from the group policy.
profileMgmt	AnyConnect Management Tunnel VPN

Example:

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

To remove one of the modules, re-send the command specifying only the module values you want to keep. For example, this command removes the websecurity module:

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

Step 5 Save the running configuration to flash.

After successfully saving the new configuration to flash memory, you receive the message [OK] and the ASA returns you to this prompt hostname(config-group-webvpn)#

write memory

HostScan/Secure Firewall Posture Related Documentation

Once HostScan/Secure Firewall Posture gathers the posture credentials from the endpoint computer, you will need to understand subjects like configuring dynamic access policies and using LUA expressions to make use of the information.

These topics are covered in detail in these documents: Cisco Adaptive Security Device Manager Configuration Guides. See also the Cisco *Secure Client (including AnyConnect) Administrator Guide* for more information about how HostScan/Secure Firewall Posture works with AnyConnect Client.

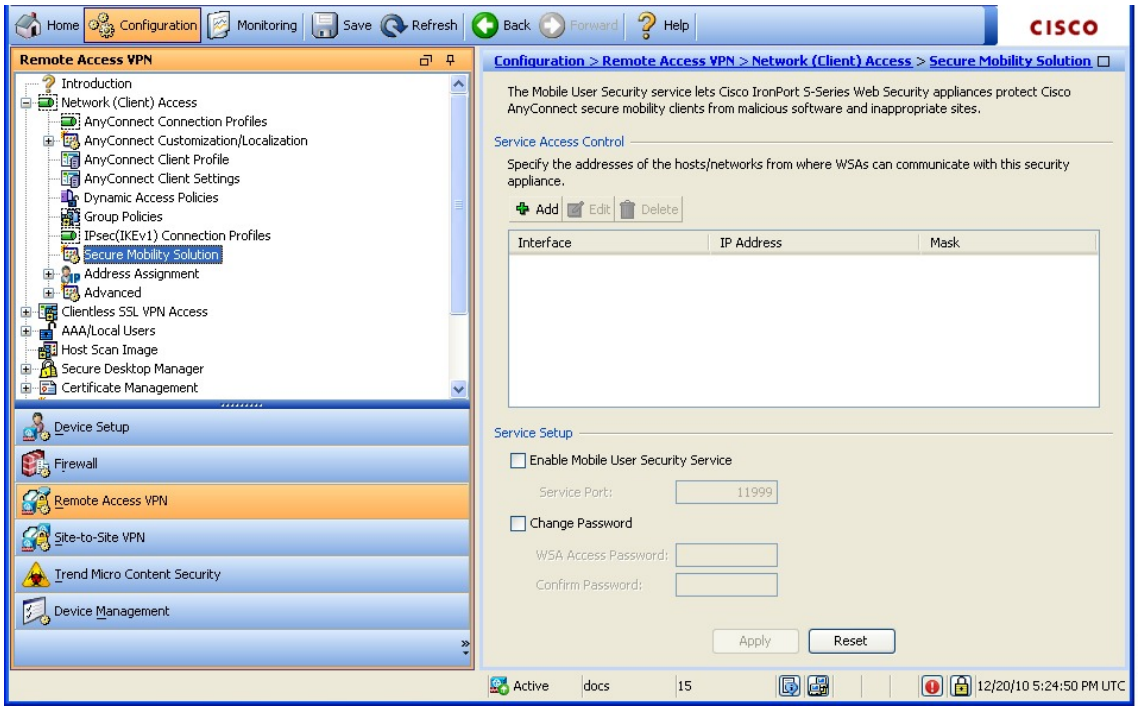
Secure Client Solution

Secure Client protects corporate interests and assets from Internet threats when employees are mobile. Secure Client lets Cisco IronPort S-Series Web Security appliances scan Secure Clients to ensure that clients are protected from malicious software and/or inappropriate sites. The client periodically checks to ensure that Cisco IronPort S-Series Web Security appliance protection is enabled.

Note This feature requires a release of the Cisco IronPort Web Security appliance that provides Secure Client licensing support for the Secure Client. It also requires an AnyConnect Client release that supports the Secure Client feature. AnyConnect 3.1 and higher does not support this feature.

To configure secure mobility solutions, choose **Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution**.

Figure 6: Mobile User Security Window



- Service Access Control—Specifies from which host or network address the WSAs can communicate.
  - Add—Opens the Add MUS Access Control Configuration dialog box for the selected connection.
  - Edit—Opens the Edit MUS Access Control Configuration dialog box for the selected connection.
  - Delete—Removes the selected connection from the table. There is no confirmation or undo.
- Enable Mobile User Security Service—Starts the connection with the client through the VPN. If enabled, you are required to enter a password, used by the WSA when contacting the ASA. If no WSA is present, the status is disabled.
- Service Port—If you choose to enable the service, specify which port number for the service to use. The port must be between 1 and 65535 and must match the corresponding value provisioned into the WSA with the management system. The default is 11999.
- Change Password—Enables you to change the WSA access password.
- WSA Access Password—Specify the shared secret password required for authentication between the ASA and WSA. This password must match the corresponding password provisioned into the WSA with the management system.
- Confirm Password—Re-enter the specified password.
- Show WSA Sessions—Allows you to view session information of WSAs connected to the ASA.The host IP address of the WSA that is connected (or has been connected) and the duration of the connection is returned in a dialog box.

Add or Edit MUS Access Control

The Add or Edit MUS Access Control dialog box under Configuration > Remote Access VPN > Network (Client) Access > Secure Mobility Solution configures Mobile User Security (MUS) access for AnyConnect Clients.

- Interface Name—Use the drop-down list to choose which interface name you are adding or editing.
- IP Address—Enter either an IPv4 or IPv6 address.
- Mask—Use the drop-down list to choose the appropriate mask.

AnyConnect Client Customization and Localization

You can customize the AnyConnect VPN client to display your own corporate image to remote users. The following fields under AnyConnect Client Customization/Localization allow you to import the following types of customized files:

- **Resources**—Modified GUI icons for the AnyConnect Client.
- **Binary**—Executable files to replace the AnyConnect Client installer. This includes GUI files, plus the VPN client profile, scripts and other client files.
- **Script**—Scripts that will run before or after AnyConnect Client makes a VPN connection.
- **GUI Text and Messages**—Titles and messages used by the AnyConnect Client.
- **Customized Installer**—Transforms that modify the client installation.
- **Localized Installer**—Transforms that change the language used by the client.

Each dialog provides the following actions:

- **Import** launches the Import AnyConnect Client Customization Objects dialog, where you can specify a file to import as an object.
- **Export** launches the Export AnyConnect Client Customization Objects dialog, where you can specify a file to export as an object.
- **Delete** removes the selected object.



Note This feature is not supported in multiple-context mode.

AnyConnect Client Customization and Localization, Resources

The filenames of the custom components that you import must match the filenames used by the AnyConnect Client GUI, which are different for each operating system and are case sensitive for Mac and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as company_logo.png. If you import it as a different filename, the AnyConnect Client installer does not change

the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.

If you import an image as a resource file (such as company_logo.bmp), the image you import customizes AnyConnect Client until you reimport another image using the same filename. For example, if you replace company_logo.bmp with a custom image, and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

AnyConnect Client Customization and Localization, Binary and Script

AnyConnect Client Customization/Localization, Binary

For Windows, Linux, or Mac (PowerPC or Intel-based) computers, you can deploy your own client that uses the AnyConnect Client API. You replace the AnyConnect Client GUI and the AnyConnect Client CLI by replacing the client binary files.

Fields for the **Import** dialog:

- **Name** Enter the name of the AnyConnect Client file that you are replacing.
- **Platform** Select the OS platform that your file runs on.
- **Select a file** The filename does not need to be the same as the name of the imported file.

AnyConnect Client Customization/Localization, Script

For complete information about deploying scripts, and their limitations and restrictions, see the AnyConnect VPN module of Cisco Secure Client Administrators Guide.

Fields for the **Import** dialog:

- **Name**—Enter a name for the script. Be sure to specify the correct extension with the name. For example, myscript.bat.
- **Script Type**—Choose when to run the script.

  AnyConnect Client adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script on the ASA. When the client connects, the ASA downloads the script to the proper target directory on the remote computer, removing the scripts_ prefix and leaving the remaining OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the ASA as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.

  To ensure the scripts run reliably, configure all ASAs to deploy the same scripts. If you want to modify or replace a script, use the same name as the previous version and assign the replacement script to all of the ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- **Platform**—Select the OS platform that your file runs on.
- **Select a file**—The filename does not need to be the same as the name you provided for the script.

ASDM imports the file from any source file, creating the new name you specify for Name.

AnyConnect Client Customization and Localization, GUI Text and Messages

You can edit the default translation table, or create new ones, to change the text and messages displayed on the AnyConnect Client GUI. This pane also shares functionality with the Language Localization pane. For more extensive language translation, go to **Configuration > Remote Access VPN > Language Localization**.

In addition to the usual buttons on the top toolbar, this pane also has an **Add** button, and a Template area with extra buttons.

Add—The Add button opens a copy of the default translation table, which you can edit directly, or save. You can choose the language of the saved file, and edit the language of the text inside the file later.

When you customize messages in the translation table, do not change msgid. Change the text in msgstr.

Specify a language for the template. The template becomes a translation table in cache memory with the name you specify. Use an abbreviation that is compatible with the language options for your browser. For example, if you are creating a table for the Chinese language, and you are using IE, use the abbreviation *zh,* that is recognized by IE.

Template Section

- Click Template to expand the template area, which provides access to the default English translation table.
- Click **View** to view, and optionally save, the default English translation table
- Click **Export** to save a copy of the default English translation table without looking at it.

AnyConnect Client Customization and Localization, Customized Installer Transforms

You can perform more extensive customizing of the AnyConnect Client GUI (Windows only) by creating your own transform that deploys with the client installer program. You import the transform to the ASA, which deploys it with the installer program.

Windows is the only valid choice for applying a transform. For more information about transforms, see the *Cisco Secure Client Administration Guide*.

AnyConnect Client Customization and Localization, Localized Installer Transforms

You can translate messages displayed by the client installer program with a transform. The transform alters the installation, but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

AnyConnect Client Custom Attributes

Custom attributes are sent to and used by the AnyConnect Client to configure features such as those below. A custom attribute has a type and a named value. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies. For information on configuring these custom attributes, refer to Configure

Secure Client Custom Attributes in an Internal Group Policy. Create and set custom attributes for many different uses:

- **DSCPPreservationAllowed**: To enable DSCP Preservation—Setting this custom attribute controls Differentiated Services Code Point (DSCP) on Windows or Mac operating system platforms for DTLS connection. It allows devices to prioritize latency sensitive traffic and marks prioritized traffic to improve outbound connection quality. For additional information, see the *Enable DSCP Preservation* section in the Cisco Secure Client Administration Guide.

  Values—True/False: By default AnyConnect Client performs DSCP preservation (True). To disable it, set the custom attribute value to false on the headend and reinitiate the connection.

- **DeferredUpdateAllowed or DeferredUpdateAllowed_ComplianceModule**: To enable deferred update on an ASA—If these custom attributes are configured, then when a client update is available, AnyConnect Client opens a dialog asking the user if they would like to update or to defer. For additional information, see Enable AnyConnect Client Deferred Upgrade or *Configure Deferred Update on an ASA* in the Cisco Secure Client Administration Guide .

  Values—True/False: True enables deferred update. If deferred update is disabled (false), the following settings are ignored.

  - **DeferredUpdateMinimumVersion_ComplianceModule or DeferredUpdateMinimumVersion**—Minimum version of AnyConnect Client that must be installed for updates to be deferrable.

    Values—x.x.x, with default of 0.0.0

  - **DeferredUpdateDismissTimeout**—Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. Applies only when a deferred update prompt is displayed.

    Values—0 to 300 seconds. Default 150 seconds.

  - **DeferredUpdateDismissResponse**—Action to take when DeferredUpdateDismissTimeout occurs.

    Values—Defer or update. Default is update.

- **dynamic-split-exclude-domains <attribute name> <list of domains> or dynamic-split-include-domains <attribute name> <list of domains>**: To enable dynamic split tunneling—By creating this custom attribute, you can dynamically split exclude tunneling after tunnel establishment based on the host DNS domain name. By adding dynamic-split-exclude-domains, you can enter cloud or web services that need access by the client from outside the VPN tunnel. For additional information, see *About Dynamic Split Tunneling* in the Cisco Secure Client Administration Guide.

  Values—The attribute name is whatever name you choose. For example, anyconnect-custom-data dynamic-split-exclude-domains excludedomains webex.com, ciscospark.com.

- **managementTunnelAllAllowed**: To enable management VPN tunnel—Management VPN tunnel requires split include tunneling configuration, by default, to avoid impacting user-initiated network communication (since it is meant to be transparent).

  Values—true/false. To override this behavior, set both attribute name and value to *true* . AnyConnect Client then proceeds with the management tunnel connection, if the configuration is one of tunnel-all, split-exclude, split-include, or bypass for both IP protocols.

- **UseLocalProfileAsAlternative**: If you want to distribute a profile out-of-band (using SCCM, MDM, SecureX Cloud Management, or the like) without configuring a Cisco Secure Client Profile (previously known as an AnyConnect profile) on the Secure Firewall ASA, you can use the *UseLocalProfileAsAlternative* custom attribute. When you configure this custom attribute, the client uses

the local (on disk) Cisco Secure Client profile for its settings and preferences (rather than the usual defaults). Refer to Predeploying Cisco Secure Client in the administration guide for additional information.

Establishing the session using the local profile only occurs when 1) *UseLocalProfileAsAlternative* is set to enabled, and 2) if an ASA group policy profile is not configured. If you configure this custom attribute and do not undo or remove the Cisco Secure Client profile from the Group Policy configuaration on the ASA, the Cisco Secure Client Profile configured on the Group Policy will be maintained and used for each connection, where the custom attribute setting will be ignored.

Name—disabled/enabled

Values—true/false

- **no-dhcp-server-route**: To set public DHCP server route—This custom attribute allows local DHCP traffic to flow in the clear when Tunnel All Network is configured. AnyConnect Client adds a specific route to the local DHCP server when the AnyConnect Client connects and applies an implicit filter on the LAN adapter of the host machine, blocking all traffic for that route except DHCP traffic. For additional information, see the *Set Public DHCP Server Route* section in the Cisco Secure Client Administration Guide.

  Values—true/false. The no-dhcp-server-route custom attribute must be present and set to true to avoid creating the public DHCP server route upon tunnel establishment.

- **circumvent-host-filtering**: To configure Linux to support excluded subnets—Sets Linux to support exclude subnets when Tunnel Network List Below is configured for split tunneling. For additional information, see Configure Linux to Support Excluded Subnets, on page 74.

  Values—true/false. Set it to true.

- **tunnel-from-any-source**—(Linux only) AnyConnect Client permits packets with any source address in Split-Include or Split-Exclude tunnel mode. It could allow network access inside VM instance or Docker container.

Note Networks used by VM/Docker must be excluded from the tunnel initially.

- **perapp**—The VPN connection is used for a specific set of apps on the mobile device (Android or Apple iOS only). Refer to the Create Per App Custom Attributes section in the *Cisco Secure Client Administration Guide* for additional information.

  Values—Add one or more values by copying the BASE64 format from the policy tool and pasting it here.

To further complete the use of these features, most of the defined custom attributes have to be associated to a certain group policy in the **Configuration > Remote Access VPN > Network (Client) Access > Group Polices** > menu.

IPsec VPN Client Software

Note **The VPN Client is end-of-life and end-of-support.** For information about configuring the VPN client, see the ASDM documentation for ASA version 9.2. **We recommend that you upgrade to the AnyConnect Secure Mobility Client.**

Zone Labs Integrity Server

The **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Zone Labs Integrity Server** panel lets you configure the ASA to support a Zone Labs Integrity Server. This server is part of the Integrity System, a system designed to enforce security policies on remote clients entering the private network. In essence, the ASA acts as a proxy for the client PC to the Firewall Server and relays all necessary Integrity information between the Integrity client and the Integrity server.

Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the ASA and then reestablish the client VPN session.

- **Server IP address**—Type the IP address of the Integrity Server. Use dotted decimal notation.
- **Add**—Adds a new server IP address to the list of Integrity Servers. This button is active when an address is entered in the Server IP address field.
- **Delete**—Deletes the selected server from the list of Integrity Servers.
- **Move Up**—Moves the selected server up in the list of Integrity Servers. This button is available only when there is more than one server in the list.
- **Move Down**—Moves the selected server down in the list of Integrity Servers. This button is available only when there is more than one server in the list.
- **Server Port**—Type the ASA port number on which it listens to the active Integrity server. This field is available only if there is at least one server in the list of Integrity Servers. The default port number is 5054, and it can range from 10 to 10000. This field is only available when there is a server in the Integrity Server list.
- **Interface**—Choose the interface ASA interface on which it communicates with the active Integrity Server. This interface name menu is only available when there is a server in the Integrity Server list.
- **Fail Timeout**—Type the number of seconds that the ASA should wait before it declares the active Integrity Server to be unreachable. The default is 10 and the range is from 5 to 20.
- **SSL Certificate Port**—Specify the ASA port to be used for SSL Authorization. The default is port 80.
- **Enable SSL Authentication**—Check to enable authentication of the remote client SSL certificate by the ASA. By default, client SSL authentication is disabled.

- **Close connection on timeout**—Check to close the connection between the ASA and the Integrity Server on a timeout. By default, the connection remains open.
- **Apply**—Click to apply the Integrity Server setting to the ASA running configuration.
- **Reset**—Click to remove Integrity Server configuration changes that have not yet been applied.

ISE Policy Enforcement

The Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access and guest access, support bring your own device (BYOD) initiatives, and enforce usage policies in conjunction with Cisco TrustSec.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is not required to apply access control lists (ACLs) for each VPN session established with the ASA.

ISE policy enforcement is supported on the following VPN clients:

- IPSec
- AnyConnect Client
- L2TP/IPSec

The system flow is as follows:

1. An end user requests a VPN connection.
2. The ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network.
3. An accounting start message is sent to the ISE to register the session.
4. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA.
5. The ISE sends a policy update to the ASA via a CoA “policy push.” This identifies a new user ACL that provides increased network access privileges.



Note Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Configure ISE Change of Authorization

Configuring ISE Change of Authorization involves creating a server group containing the ISE RADIUS servers, then using that server group in remote access VPN configuration profiles (tunnels).

Procedure

Step 1 Configure the RADIUS AAA server group for the ISE servers.

The following procedure explains the minimum configuration. You can adjust other settings for the group as desired. Most settings have defaults appropriate for most networks. See the general configuration guide for complete information on configuring RADIUS AAA server groups.

a) Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.
b) Click **Add** in the **AAA Server Groups** area.
c) Enter a name for the group in the **AAA Server Group** field.
d) Choose the RADIUS server type from the **Protocol** drop-down list.
e) Select **Enable interim accounting update** and **Update Interval** to enable the periodic generation of RADIUS interim-accounting-update messages.

ISE maintains a directory of active sessions based on the accounting records that it receives from NAS devices like the ASA. However, if ISE does not receive any indication that the session is still active (accounting message or posture transactions) for a period of 5 days, it will remove the session record from its database. To ensure that long-lived VPN connections are not removed, configure the group to send periodic interim-accounting-update messages to ISE for all active sessions.

You can change the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120.

f) Select **Enable dynamic authorization**.

This option enables the RADIUS Dynamic Authorization (ISE Change of Authorization, CoA) services for the AAA server group. When you use the server group in a VPN tunnel, the RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from ISE. Do not change the port (1700) unless your ISE server is configured to use a different port. The valid range is 1024 to 65535.

g) If you do not want to use ISE for authentication, select **Use authorization only mode**.

This option indicates that when this server group is used for authorization, the RADIUS Access Request message will be built as an “Authorize Only” request as opposed to the configured password methods defined for the AAA server. If you do configure a common password for the RADIUS server, it will be ignored.

For example, you would use authorize-only mode if you want to use certificates for authentication rather than this server group. You would still use this server group for authorization and accounting in the VPN tunnel.

h) Click **OK** to save the server group.
i) With the server group selected, click **Add** in the **Servers in selected group** list to add the ISE RADIUS servers to the group.

Following are the key attributes. You can adjust the defaults for other settings as needed.

- **Interface Name**—The interface through which you can reach the ISE server.
- **Server Name or IP Address**—The ISE server's hostname or IP address.

- (Optional.) **Server Secret Key**—The key for encrypting the connection. If you do not configure a key, the connection is not encrypted (plain text). The key is a case-sensitive, alphanumeric string of up to 127 characters that is the same value as the key on the RADIUS server.

j) Click **OK** to add the server to the group.

Add any additional ISE servers to the server group.

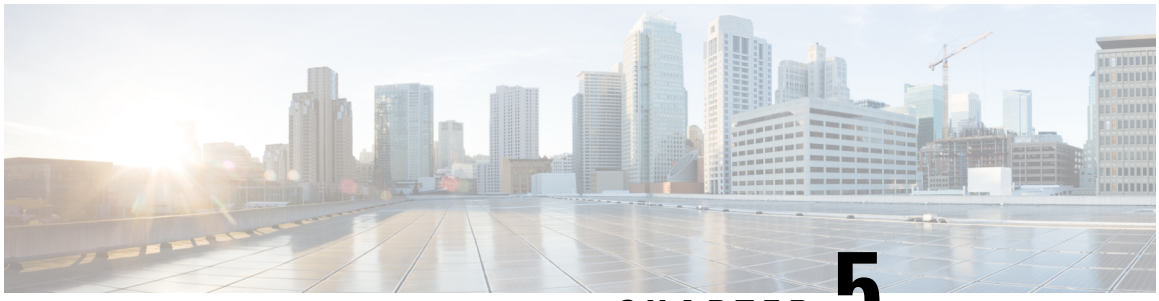
Step 2 Update the configuration profiles for remote access VPN to use the ISE server group.

The following steps cover the ISE-related configuration options only. There are other options you need to configure to create a functional remote access VPN. Follow the instructions elsewhere in this guide for implementing remote access VPN.

a) Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access**AnyConnect Client **Connection Profiles**.
b) In the **Connection Profiles** table, add or edit a profile.
c) On the **Basic** page, configure the authentication method.

- If you are using the ISE servers for authentication, select **AAA** for **Authentication** > **Method**, then select the ISE AAA server group.
- If you configured the ISE server group for authorization only, select a different authentication method, for example, **Certificate**.

d) On the **Advanced** > **Authorization** page, select the ISE server group for **Authorization Server Group**.
e) On the **Advanced** > **Accounting** page, select the ISE server group.
f) Click **OK** to save your changes.



CHAPTER 5

IP Addresses for VPNs

- Configure an IP Address Assignment Policy, on page 151
- Configure Local IP Address Pools, on page 153
- Configure DHCP Addressing, on page 155
- Assign IP Addresses to Local Users, on page 156

Configure an IP Address Assignment Policy

The ASA can use one or more of the following methods for assigning IP addresses to remote access clients. If you configure more than one address assignment method, the ASA searches each of the options until it finds an IP address. By default, all methods are enabled.

- Use authentication server — Retrieves addresses from an external authentication, authorization, and accounting server on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method. You can configure AAA servers in the Configuration > AAA Setup pane.This method is available for IPv4 and IPv6 assignment policies.
- Use DHCP — Obtains IP addresses from a DHCP server. If you want to use DHCP, you must configure a DHCP server. You must also define the range of IP addresses that the DHCP server can use. If you use DHCP, configure the server in the Configuration > Remote Access VPN > DHCP Server pane. This method is available for IPv4 assignment policies.
- **Use an internal address pool —** Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, configure the IP address pools in Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools pane. This method is available for IPv4 and IPv6 assignment policies.
  - Allow the reuse of an IP address so many minutes after it is released—Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default, this is unchecked, meaning the ASA does not impose a delay. If you want one, check the box and enter the number of minutes in the range 1 - 480 to delay IP address reassignment.This configurable element is available for IPv4 assignment policies.

Note When you configure both a DHCP server and a local IP address pool for address assignment, automatic fallback to the local pool (if the DHCP server is unavailable) works only for SSL-based remote access VPN connections.

For IPsec-based remote access VPN connections, this fallback may not complete in time if the DHCP server is unreachable, which can cause the connection to fail.

To avoid connection issues with IPsec-based remote access VPN, do one of the following:

- Make sure the DHCP server is reachable, or
- Use only a local IP address pool for address assignment.

Use one of the following methods to specify a way to assign IP addresses to remote access clients.

Configure IP Address Assignment Options

Procedure

Step 1 Select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Assignment Policy**

Step 2 In the IPv4 Policy area, check the address assignment method to enable it or uncheck the address assignment method to disable it. These methods are enabled by default:

- Use Authentication server. Enables the use of a Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
- Use DHCP. Enables the use of a Dynamic Host Configuration Protocol (DHCP) server you have configured to provide IP addresses.
- Use internal address pools: Enables the use of a local address pool configured on the ASA.

If you enable **Use internal address pools**, you can also enable the reuse of an IPv4 address after it has been released. You can specify a range of minutes from 0-480 after which the IP v4 address can be reused.

Step 3 In the IPv6 Policy area, check the address assignment method to enable it or uncheck the address assignment method to disable it. These methods are enabled by default:

- Use Authentication server. Enables the use of a Authentication Authorization and Accounting (AAA) server you have configured to provide IP addresses.
- Use internal address pools: Enables the use of a local address pool configured on the ASA.

Step 4 Click **Apply**.

Step 5 Click **OK**.

View Address Assignment Methods

Procedure

Select **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.**

Configure Local IP Address Pools

To configure IPv4 or IPv6 address pools for VPN remote access tunnels, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add/Edit IP Pool**. To delete an address pool, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools**. Select the address pool you want to delete and click **Delete**.

The ASA uses address pools based on the connection profile or group policy for the connection. The order in which you specify the pools is important. If you configure more than one address pool for a connection profile or group policy, the ASA uses them in the order in which you added them to the ASA.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Configure Local IPv4 Address Pools

The IP Pool area shows the configured address pools by name with their IP address range, for example: 10.10.147.100 to 10.10.147.177. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Procedure

Step 1 **Select Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.**

Step 2 To add an IPv4 address, click **Add > IPv4 Address pool**. To edit an existing address pool, choose the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box enter this information:

- Pool Name—Enter the name of the address pool. It can be up to 64 characters
- Starting Address—Enter the first IP address available in each configured pool. Use dotted decimal notation, for example: 10.10.147.100.
- Ending Address—Enter the last IP address available in each configured pool. User dotted decimal notation, for example: 10.10.147.177.

- Subnet Mask—Identifies the subnet on which this IP address pool resides.

Step 4 Click **Apply**.

Step 5 Click **OK**.

Configure Local IPv6 Address Pools

The IP Pool area shows the configured address pools by name with a starting IP address range, the address prefix, and the number of addresses configurable in the pool. If no pools exist, the area is empty. The ASA uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Procedure

Step 1 **Select Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Address Pools.**

Step 2 To add an IPv6 address, click **Add** > **IPv6 Address pool**. To edit an existing address pool, choose the address pool in the address pool table and click **Edit**.

Step 3 In the Add/Edit IP Pool dialog box enter this information:

- Name—Displays the name of each configured address pool.

  Starting IP Address—Enter the first IP address available in the configured pool. For example: 2001:DB8::1.

- Prefix Length— Enter the IP address prefix length in bits. For example 32 represents /32 in CIDR notation. The prefix length defines the subnet on which the pool of IP addresses resides.

- Number of Addresses—Identifies the number of IPv6 addresses, starting at the Starting IP Address, that are in the pool.

Step 4 Click **Apply**.

Step 5 Click **OK**.

Assign Internal Address Pools to Group Policies

The Add or Edit Group Policy dialog box lets you specify address pools, tunneling protocols, filters, connection settings, and servers for the internal Network (Client) Access group policy being added or modified. For each of the fields in this dialog box, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all the attributes in this dialog box.

You can configure both IPv4 and IPv6 address pools for the same group policy. If both versions of IP addresses are configured in the same group policy, clients configured for IPv4 will get an IPv4 address, clients configured

for IPv6 will get an IPv6 address, and clients configured for both IPv4 and IPv6 addresses will get both an IPv4 and an IPv6 address.

Procedure

Step 1 Connect to the ASA using ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.

Step 2 Create a new group policy or the group policy you want to configure with an internal address pool and click Edit.

The General attributes pane is selected by default in the group policy dialog.

Step 3 Use the Address Pools field to specify an IPv4 address pool for this group policy. Click Select to add or edit an IPv4 address pool.

Step 4 Use the IPv6 Address Pools field to specify an IPv6 address pools to use for this group policy. Click Select to add or edit a IPv6 address pool.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Configure DHCP Addressing

To use DHCP to assign addresses for VPN clients, you must first configure a DHCP server and the range of IP addresses that the DHCP server can use. Then you define the DHCP server on a connection profile basis. Optionally, you can also define a DHCP network scope in the group policy associated with a connection profile or username.

The following example defines the DHCP server at 172.33.44.19 for the connection profile named **firstgroup**. The example also defines a DHCP network scope of 10.100.10.1 for the group policy called **remotegroup**. (The group policy called remotegroup is associated with the connection profile called firstgroup). If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

Before you begin

You can only use an IPv4 address to identify a DHCP server to assign client addresses. In addition, DHCP options are not forwarded to users, they receive an address assignment only.

Procedure

Step 1 Configure your DHCP servers.

You cannot assign IPv6 addresses to AnyConnect Clients using a DHCP server.

a) Verify that DHCP is enabled on **Configuration** > **Remote Access VPN** > **Network (Client) Access** > > **Address Assignment** > **Assignment Policy**.

b) Configure your DHCP servers by selecting **Configuration** > **Remote Access VPN** > **DHCP Server**.

Step 2 Define the DHCP server in the connection profile.

a) Select **Configuration** > **Remote Access VPN** > **Network (Client) Access > AnyConnect Connection Profiles**.
b) In the Connection Profiles Area click **Add** or **Edit**.
c) Click **Basic** in the configuration tree for the connection profile.
d) In the Client Address Assignment area, enter the IPv4 address of the DHCP server you want to use to assign IP addresses to clients. For example, **172.33.44.19**.

Step 3 Edit the group-policy associated with the connection profile to define the DHCP scope.

a) Select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.
b) Double-click the group policy you want to edit.
c) Click **Server**in the configuration tree.
d) Expand the **More Options** area by clicking the down arrow.
e) Uncheck DHCP Scope **Inherit** and define the DHCP scope.

   If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

   If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

   To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

   We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

f) Click **OK**.
g) Click **Apply**.

Assign IP Addresses to Local Users

Local user accounts can be configured to use a group policy, and some AnyConnect Client attributes can also be configured. These user accounts provide fallback if the other sources of IP address fail, so administrators will still have access.

Before you begin

To add or edit a user, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users** and click **Add** or **Edit**.

By default, the **Inherit** check box is checked for each setting on the Edit User Account screen, which means that the user account inherits the value of that setting from the default group policy, DfltGrpPolicy.

To override each setting, uncheck the **Inherit** check box, and enter a new value. The detailed steps that follow describe the IP address settings. See Configure VPN Policy Attributes for a Local User, on page 89 for full configuration details.

Procedure

Step 1 Start ASDM and choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users**.

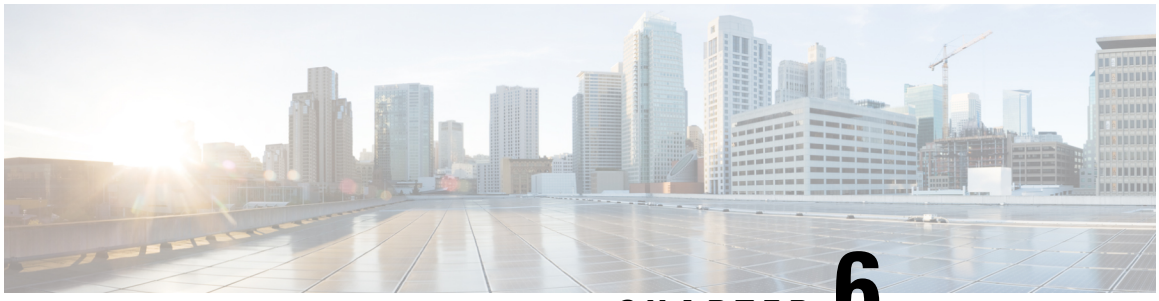
Step 2 Choose the user you want to configure and click **Edit**.

Step 3 In the left pane, click **VPN Policy**.

Step 4 To set a dedicated IPv4 address for this user, enter an IPv4 address and subnet mask in the **Dedicated IPv4 Address (Optional)** area.

Step 5 To set a dedicated IPv6 address for this user, enter an IPv6 address with an IPv6 prefix in the **Dedicated IPv6 Address (Optional)** area. The IPv6 prefix indicates the subnet on which the IPv6 address resides.

Step 6 Click**Apply** to save the changes to the running configuration.



CHAPTER 6

Dynamic Access Policies

This chapter describes how to configure dynamic access policies.

- About Dynamic Access Policies, on page 159
- Licensing for Dynamic Access Policies, on page 161
- Configure Dynamic Access Policies, on page 161
- Configure AAA Attribute Selection Criteria in a DAP, on page 165
- Configure Endpoint Attribute Selection Criteria in a DAP, on page 168
- Create Additional DAP Selection Criteria in DAP Using LUA, on page 180
- Configure DAP Access and Authorization Policy Attributes, on page 186
- Configure SAML Authorization Using DAP, on page 190
- Perform a DAP Trace, on page 191
- Examples of DAPs, on page 192

About Dynamic Access Policies

VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP) on the ASA let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the ASA grants access to a particular user for a particular session based on the policies you define. The ASA generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

The DAP system includes the following components that require your attention:

- DAP Selection Configuration File—A text file containing criteria that the ASA uses for selecting and applying DAP records during session establishment. Stored on the ASA. You can use ASDM to modify it and upload it to the ASA in XML data format. DAP selection configuration files include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding and URL lists.

- DfltAccess Policy—Always the last entry in the DAP summary table, always with a priority of 0. You can configure Access Policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes. You cannot delete the DfltAccessPolicy, and it must be the last entry in the summary table.

Refer to the *Dynamic Access Deployment Guide* (https://supportforums.cisco.com/docs/DOC-1369) for additional information.

DAP Support of Remote Access Protocols and Posture Assessment Tools

The ASA obtains endpoint security attributes by using posture assessment tools that you configure. These posture assessment tools include the Secure Firewall Posture Module, the independent HostScan/Secure Firewall Posture package, and NAC.

The following table identifies each of the remote access protocols DAP supports, the posture assessment tools available for that method, and the information that tool provides.

Supported Remote Access Protocol	**Secure Firewall Posture Module** **Host Scan package** **Secure Firewall Posture**	**Secure Firewall Posture Module** **HostScan package** **Secure Firewall Posture**	**NAC**	**Cisco NAC Appliance**
	Returns file information, registry key values, running processes, operating system	Returns anti-malware and personal firewall software information	Returns NAC status	Returns VLAN Type and VLAN IDs
IPsec VPN	No	No	Yes	Yes
Cisco AnyConnect VPN	Yes	Yes	Yes	Yes
Clientless (browser-based) SSL VPN	Yes	Yes	No	No
PIX Cut-through Proxy (posture assessment not available)	No	No	No	No

Remote Access Connection Sequence with DAPs

The following sequence outlines a typical remote access connection establishment.

1. A remote client attempts a VPN connection.
2. The ASA performs posture assessment, using configured NAC and HostScan/Secure Firewall Posture values.

3. The ASA authenticates the user via AAA. The AAA server also returns authorization attributes for the user.
4. The ASA applies AAA authorization attributes to the session, and establishes the VPN tunnel.
5. The ASA selects DAP records based on the user AAA authorization information and the session posture assessment information.
6. The ASA aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The ASA applies the DAP policy to the session.

Licensing for Dynamic Access Policies



Note This feature is not available on No Payload Encryption models.

Dynamic access policies (DAP) require one of the following licenses:

- AnyConnect Apex—To use all DAP features.
- AnyConnect Plus—For operating system and operating system/AnyConnect Client version checking only.

Related Topics

Add AnyConnect Client Endpoint Attributes to a DAP, on page 171

Configure Dynamic Access Policies

Before you begin

- Other than where noted, you must install HostScan/Secure Firewall Posture before configuring DAP endpoint attributes.
- If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.
- Due to Java Web Start security issues, you may find that you are unable to populate Advanced Endpoint Attribute with configured values if you use webvpn based configuration on the device. To overcome this issue, either use ASDM Desktop application or add the AEA related URL(s) as the exception in the Java Security.
- Before configuring File, Process, and Registry endpoint attributes, configure File, Process, and Registry Basic HostScan/Secure Firewall Posture attributes. For instructions, navigate within ASDM to the appropriate UI screen and click **Help**.
- DAP supports only ASCII characters.

Procedure

Step 1 Start ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access Dynamic Access Policies**.

Note
If an **Incompatible** action button is displayed below the Add, Edit and Delete action, there has been an attempt to upgrade HostScan to a version (4.6.x or later) that has had internal library updates that make it incompatible with your existing DAP policies (created when using HostScan 4.3.x or earlier). You MUST carry out a one-time migration procedure to adapt your configuration.

The appearance of the **Incompatible** action indicates that the HostScan upgrade has been initiated and you now need to migrate your configuration. Refer to the AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide for detailed instructions.

Step 2 To include certain antimalware or personal firewall endpoint attributes, click the **configuration** link near the top of the pane. This link does not display if you have previously enabled both of these features.

Step 3 View the list of previously configured DAPs.

The following fields are shown in the table:

- ACL Priority—Displays the priority of the DAP record's ACL.

  The ASA uses this value to logically sequence the ACLs when aggregating the network and web-type ACLs from multiple DAP records. The ASA orders the records from highest to lowest priority number, with lowest at the bottom of the table. Higher numbers have a higher priority, that is a DAP record with a value of 4 has a higher priority than a record with a value of 2. You cannot manually sort them.

- Name—Displays the name of the DAP record.
- Network ACL List—Displays the name of the firewall ACL that applies to the session.
- Web-Type ACL List—Displays the name of the SSL VPN ACL that applies to the session.
- Description—Describes the purpose of the DAP record.

Step 4 Click **Add** or **Edit** to Add or Edit a Dynamic Access Policy, on page 163.

Step 5 Click **Apply** to save your DAP configuration.

Step 6 Search for a Dynamic Access Policy (DAP) by using the **Find** field.

Start typing in the field and the tool will search the beginning characters of every field of the DAP table for a match. You can use wild cards to expand your search.

For example typing **`sal`** in the **Find** field matches a DAP named `Sales` but not a DAP named `Wholesalers`. If you type **`*sal`** in the **Find** field, the search finds the first instance of either **`Sales`** or **`Wholesalers`** in the table.

Step 7 Test Dynamic Access Policies, on page 165 to verify your configuration.

Note The priorities in DAP records only apply to the ACLs that are aggregated from them when creating the composite ACL list. ACLs are aggregated in order of priority, and are evaluated in order, from highest to lowest.

Key differences between DAP records and ACLs:

- DAP records control whether a connection is allowed. ACLs control what traffic is permitted once connected.
- Multiple DAP records are all evaluated simultaneously, while multiple ACLs are aggregated into a single ACL. The ACLs are evaluated sequentially and stop at the first match.

Add or Edit a Dynamic Access Policy

Procedure

Step 1 Start ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** or **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add** or **Edit.**

Step 2 Provide a name (required) and a description (optional) of this dynamic access policy.

- The **Policy Name** is a string of 4 through 32 characters, no spaces allowed.
- You are allowed a maximum of 80 characters in the DAP **Description** field.

Step 3 In the **ACL Priority** field, set a priority for the DAP record's ACL.

The security appliance aggregates ACLs in the order you set here, with the highest number having the highest priority. Values of 0 to 2147483647 are valid. The default value is 0.

Step 4 Specify your selection criteria for this DAP:

a) In the Selection Criteria pane, use the ANY/ALL/NONE drop-down list (unlabeled) to choose whether a user must have any, all, or none of the AAA attribute values you configure to use this dynamic access policy, as well as satisfying every endpoint attribute.

Duplicate entries are not allowed. If you configure a DAP record with no AAA or endpoint attributes, the ASA always selects it since all selection criteria are satisfied.

b) Click **Add** or **Edit** in the AAA Attributes field to Configure AAA Attribute Selection Criteria in a DAP, on page 165.

c) Click **Add** or **Edit** in the Endpoint Attributes area to Configure Endpoint Attribute Selection Criteria in a DAP, on page 168.

d) Click the **Advanced** field to #unique_177. This feature requires knowledge of the Lua programming language.

- AND/OR—Click to define the relationship between the basic selection rules and the logical expressions you enter here, that is, whether the new attributes add to or substitute for the AAA and endpoint attributes already set. The default is AND.

- Logical Expressions—You can configure multiple instances of each type of endpoint attribute. Enter free-form LUA text that defines new AAA and/or endpoint selection attributes. ASDM does not validate text that you enter here; it just copies this text to the DAP XML file, and the ASA processes it, discarding any expressions it cannot parse.

  For information about importing/exporting a *dap.xml* file, see Import and Export the DAP XML File between Two ASAs, on page 164.

Step 5 Specify the **Access/Authorization Policy Attributes** for this DAP.

Attribute values that you configure here override authorization values in the AAA system, including those in existing user, group, tunnel group, and default group records. See Configure DAP Access and Authorization Policy Attributes, on page 186.

Step 6 Click **OK**.

Import and Export the DAP XML File between Two ASAs

The Dynamic Access Policies (DAP) configuration of ASA is stored in a file called *dap.xml* on the ASA's flash memory. The file contains the DAP policies selection attributes.



Note Although you can export the *dap.xml* file, edit it (if you know about xml syntax), and re-import it back, be very careful, because you can cause ASDM to stop processing DAP records if you have misconfigured something. There is no CLI to manipulate this part of the configuration.

Use these steps to import and export the *dap.xml* file between two ASAs.

The procedure uses the example of exporting a *dap.xml* file from ASA#1 and importing in on ASA#2.

For information about handling files on ASA using the ASDM, see the *Managing Files* section of the *Cisco ASA Series General Operations ASDM Configuration Guide*.

Procedure

Step 1 Clear the *dap.xml* file on the ASA#2.

a) Save the ASA#2 configuration and *dap.xml* externally to a tftp or an ftp server.
b) Exit the ASDM for ASA#2.

Note
You can also use the **ASDM** > **Tools** > **BackUp Configurations** > **DAP Configurations** option to save the *dap.xml* file.

You can also rename or delete the *dap.xml* file on the ASA#2 flash memory.

Step 2 On the ASA#2 command prompt, enter the **clear configure dynamic-access-policy-record** command to remove the DAP record configurations.

Step 3 Export the *dap.xml* file from ASA#1 flash and import it on the ASA#2 flash.

Step 4 Use the **dynamic-access-policy-record** command to configure the DAP record entries from ASA#1 on ASA#2.

Step 5 On ASA#2 enable DAP using the **dynamic-access-policy-config activate** command.

Note
You can also relaunch the ASDM for ASA#2 to activate the DAP configuration.

Step 6 Relaunch the ASDM on ASA#2.
The new DAP policies are configured in ASA#2.

Test Dynamic Access Policies

This pane lets you test the retrieval of the set of DAP records configured on the device by specifying authorization attribute value pairs.

Procedure

Step 1 Use the Add/Edit buttons associated with the AAA Attribute and Endpoint Attribute tables to specify attribute value pairs.

The dialogs that display when you click these Add/Edit buttons are similar to those in the Add/Edit AAA Attributes and Add/Edit Endpoint Attributes dialog boxes.

Step 2 Click the **Test** button.

The DAP subsystem on the device references these values when evaluating the AAA and endpoint selection attributes for each record. The results display in the **Test Results** area.

Configure AAA Attribute Selection Criteria in a DAP

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the ASA receives from a RADIUS or LDAP server. The ASA selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The ASA can choose multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

Procedure

To configure AAA attributes as selection criteria for DAP records, in the Add/Edit AAA Attributes dialog box, set the Cisco, LDAP, or RADIUS attributes that you want to use. You can set these attributes either to = or != the value you enter. There is no limit for the number of AAA attributes for each DAP record. For detailed information about AAA attributes, see AAA Attribute Definitions, on page 168.

AAA Attributes Type—Use the drop-down list to choose Cisco, LDAP or RADIUS attributes:

- Cisco—Refers to user authorization attributes that are stored in the AAA hierarchical model. You can specify a small subset of these attributes for the AAA selection attributes in the DAP record.These include:
  - Group Policy —The group policy name associated with the VPN user session. Can be set locally on the security appliance or sent from a RADIUS/LDAP server as the IETF-Class (25) attribute. Maximum 64 characters.
  - Assigned IP Address—Enter the IPv4 address you want to specify for the policy.
  - Assigned IPv6 Address—Enter the IPv6 address you want to specify for the policy.
  - Connection Profile—The connection or tunnel group name. Maximum 64 characters.
  - Username—The username of the authenticated user. Maximum 64 characters. Applies if you are using Local, RADIUS, LDAP authentication/authorization or any other authentication type (for example, RSA/SDI), NT Domain, etc).
  - =/!=—Equal to/Not equal to.
- LDAP—The LDAP client (security appliance) stores all native LDAP response attribute value pairs in a database associated with the AAA session for the user. The LDAP client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the LDAP server. The user record attributes are read first, and always have priority over group record attributes.

  To support Active Directory group membership, the AAA LDAP client provides special handling of the LDAP memberOf response attribute. The AD memberOf attribute specifies the DN string of a group record in AD. The name of the group is the first CN value in the DN string. The LDAP client extracts the group name from the DN string and stores it as the AAA memberOf attribute, and in the response attribute database as the LDAP memberOf attribute. If there are additional memberOf attributes in the LDAP response message, then the group name is extracted from those attributes and is combined with the earlier AAA memberOf attribute to form a comma separated string of group names, also updated in the response attribute database.

  In the case where the VPN remote access session to an LDAP authentication/authorization server returns the following three Active directory groups (memberOf enumerations):

  cn=Engineering,ou=People,dc=company,dc=com

  cn=Employees,ou=People,dc=company,dc=com

  cn=EastCoastast,ou=People,dc=company,dc=com

  the ASA processes three Active Directory groups: Engineering, Employees, and EastCoast which could be used in any combination as aaa.ldap selection criteria.

  LDAP attributes consist of an attribute name and attribute value pair in the DAP record. The LDAP attribute name is syntax/case sensitive. If for example you specify LDAP attribute Department instead of what the AD server returns as department, the DAP record will not match based on this attribute setting.

  Note
  To enter multiple values in the Value field, use the semicolon (;) as the delimiter. For example:

  eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS—The RADIUS client stores all native RADIUS response attribute value pairs in a database associated with the AAA session for the user. The RADIUS client writes the response attributes to the database in the order in which it receives them. It discards all subsequent attributes with that name. This scenario might occur when a user record and a group record are both read from the RADIUS server. The user record attributes are read first, and always have priority over group record attributes.

  RADIUS attributes consist of an attribute number and attribute value pair in the DAP record.

  Note
  For RADIUS attributes, DAP defines the Attribute ID = 4096 + RADIUS ID.

  For example:

  The RADIUS attribute "Access Hours" has a Radius ID = 1, therefore DAP attribute value = 4096 + 1 = 4097.

  The RADIUS attribute "Member Of" has a Radius ID = 146, therefore DAP attribute value = 4096 + 146 = 4242.

- LDAP and RADIUS attributes include:
  - Attribute ID—Names/numbers the attribute. Maximum 64 characters.
  - Value—The attribute name (LDAP) or number (RADIUS).

    To enter multiple values in the Value field, use the semicolon (;) as the delimiter. For example:
    `eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
  - =/!=—Equal to/Not equal to.

- LDAP includes the Get AD Groups button. See Retrieve Active Directory Groups, on page 167.

Retrieve Active Directory Groups

You can query an Active Directory server for available AD groups in this pane. This feature applies only to Active Directory servers using LDAP. This button queries the Active Directory LDAP server for the list of groups the user belong to (memberOf enumerations). Use the group information to specify dynamic access policy AAA selection criteria.

AD groups are retrieved from the LDAP server using the CLI s**how-ad-groups** command in the background. The default time that the ASA waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.

You can change the level in the Active Directory hierarchy where the search begins by changing the Group Base DN in the Edit AAA Server pane. You can also change the time that the ASA waits for a response from the server in the window. To configure these features, choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Edit AAA Server**.

Note If the Active Directory server has a large number of groups, the list of AD groups retrieved (or the output of the **show ad-groups** command) may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the filter feature to reduce the number of groups reported by the server.

AD Server Group—The name of the AAA server group to retrieve AD groups.

Filter By—Specify a group or the partial name of a group to reduce the groups displayed.

Group Name—A list of AD groups retrieved from the server.

AAA Attribute Definitions

The following table defines the AAA selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do in the Advanced section of the Add/Edit Dynamic Access Policy pane.

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Cisco	aaa.cisco.grouppolicy	AAA	string	64	Group policy name on the ASA or sent from a Radius/LDAP server as the IETF-CLass (25) attribute
	aaa.cisco.ipaddress	AAA	number	-	Assigned IP address for full tunnel VPN clients (IPsec, L2TP/IPsec, SSL VPN Anyconnect module)
	aaa.cisco.tunnelgroup	AAA	string	64	Connection profile (tunnel group) name
	aaa.cisco.username	AAA	string	64	Name of the authenticated user (applies if using Local authentication/authorization)
LDAP	aaa.ldap.<*label*>	LDAP	string	128	LDAP attribute value pair
RADIUS	aaa.radius.<number>	RADIUS	string	128	Radius attribute value pair

Configure Endpoint Attribute Selection Criteria in a DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The ASA dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the ASA to choose it for a session. The ASA selects only DAP records that satisfy every condition configured.

Before you begin

- Configuring endpoint attributes as selection criteria for DAP records is part of a larger process to Configure Dynamic Access Policies, on page 161. Review this procedure before configuring endpoint attributes as selection criteria for DAPs.
- For detailed information about Endpoint attributes, see Endpoint Attribute Definitions, on page 177.
-
- For detailed information on how HostScan/Secure Firewall Posture checks for antimalware and personal firewall programs that are memory-resident, see DAP and Antimalware and Personal Firewall Programs, on page 176.

Procedure

Step 1 Click **Add** or **Edit** and add any of the following endpoint attributes as selection criteria.

You can create multiple instances of each type of endpoint attribute. There is no limit for the number of endpoint attributes for each DAP record.

- Add an Anti-Malware Endpoint Attribute to a DAP, on page 170
- Add an Application Attribute to a DAP, on page 170
- Add AnyConnect Client Endpoint Attributes to a DAP, on page 171
- Add a File Endpoint Attribute to a DAP, on page 172
- Add a Device Endpoint Attribute to a DAP, on page 173
- Add a NAC Endpoint Attribute to a DAP, on page 173
- Add an Operating System Endpoint Attribute to a DAP, on page 174
- Add a Personal Firewall Endpoint Attribute to a DAP, on page 174
- Add a Policy Endpoint Attribute to a DAP, on page 175
- Add a Process Endpoint Attribute to a DAP, on page 175
- Add a Registry Endpoint Attribute to a DAP, on page 175
- Add Multiple Certificate Authentication Attributes to DAP, on page 176

Step 2 Specify the DAP policy matching criteria.

For each of these endpoint attribute types, decide whether the DAP policy should require that the user have all instances of a type (Match all = AND, default) or only one of them (Match Any = OR).

a) Click **Logical Op.**
b) Choose **Match Any** (default) or **Match All** for each type of endpoint attribute.
c) Click **OK**.

Step 3 Return to Add or Edit a Dynamic Access Policy, on page 163.

Add an Anti-Malware Endpoint Attribute to a DAP

Before you begin

If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Anti-Malware**.

Step 2 Click the appropriate **Installed or Not Installed** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.

Step 3 Determine if you want realtime scanning enabled or disabled.

Step 4 From the **Vendor** list box, choose the name of the anti-malware vendor you are testing for.

Step 5 Check the **Product Description** check box and choose from the list box the vendor's product name you are testing for.

Step 6 Check the **Version** checkbox and set the operation field to equal to (=), not equal (!=), less than (<), greater than (>), less that or equal to (<=), or greater than or equal to (>=) the product version number you choose from the **Version** list box.

If the choice in the version list box has an x, such as 3.x, replace the x with a specific release number, for example, 3.5.

Step 7 Check the **Last Update** check box. Specify the number of days since the last update. You might want to indicate that an update should occur in less than (<) or more than (>) the number of days you enter here.

Step 8 Click **OK**.

Add an Application Attribute to a DAP

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Application**.

Step 2 In the Client Type operation field, choose equals (=) or does not eaqual (!=).

Step 3 In the Client type list box, indicate the type of remote access connection you are testing for.

Step 4 Click **OK**.

Add AnyConnect Client Endpoint Attributes to a DAP

AnyConnect Client Endpoint Attributes, also known as Mobile Posture or AnyConnect Identity Extensions (ACIDex), are used by the AnyConnect VPN client to communicate posture information to the ASA. Dynamic Access Polices use these endpoint attributes to authorize users.

These mobile posture attributes can be included in a dynamic access policy and enforced without installing HostScan/Secure Firewall Posture on the endpoint.

Some mobile posture attributes are relevant to the AnyConnect Client running on mobile devices only. Some mobile posture attributes are relevant to both AnyConnect Clients running on mobile devices and AnyConnect Client desktop clients.

Before you begin

Mobile posture requires an AnyConnect Client Mobile license and an AnyConnect Client Premium license installed on the ASA. Enterprises that install these licenses will be able to enforce DAP policies on supported mobile devices based on DAP attributes and other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose AnyConnect Client.

Step 2 Check the **Client Version** check box and set the operation field to be equal to (=), not equal to (!=), less than (<), greater than (>), less than or equal to (<=), or greater than or equal to (>=) the AnyConnect Client version number you then specify in the **Client Version** field.

You can use this field to evaluate the client version on mobile devices, such as mobile phones and tablets, or desktop and laptop devices.

Step 3 Check the **Platform** check box and set the operation field to be equal to (=), or not equal to (!=) the operating system you then choose from the **Platform** list box.

You can use this field to evaluate the operating system on mobile devices, such as mobile phones and tablets, as well as the operating system on desktop and laptop devices. Selecting a platform activates the additional attribute fields for Device Type and Device Unique ID.

Step 4 Check the **Platform Version** check box and set the operation field to be equal to (=), not equal to (!=), less than (<), greater than (>), less than or equal to (<=), or greater than or equal to (>=) the operating system version number you then specify in the **Platform Version** field.

If you want to create a DAP record that contains this attribute, be sure to also specify a Platform in the previous step.

Step 5 If you selected the Platform checkbox you can check the **Device Type** checkbox. Set the operation field to be equal to (=) or not equal to (!=) the device you then choose or enter in the **Device Type** field.

If you have a supported device which is not listed in the Device Type field, you can enter it in the Device Type field. The most reliable way to obtain the device type information is to install the AnyConnect Client on the endpoint, connect to the ASA, and perform a DAP Trace. In the DAP trace results, look for the value of **endpoint.anyconnect.devicetype**. That is the value that you need to enter in the Device Type field.

Step 6 If you selected the Platform checkbox you can check the **Device Unique ID** checkbox. Set the operation field to be equal to (=) or not equal to (!=) the device's unique ID you then specify in the **Device Unique ID** field.

The Device Unique ID distinguishes individual devices allowing you to set policies for a particular mobile device. To obtain a device's unique ID you need the device to connect to the ASA and perform a DAP trace, look for the value of **endpoint.anyconnect.deviceuniqueid**. That is the value that you need to enter in the Device Unique ID field.

Step 7 If you selected a Platform, you can add MAC addresses to the **MAC Addresses Pool** field. Set the operation field to be equal to (=) or not equal to (!=) the specified MAC addresses. Each MAC address must be in the format xx-xx-xx-xx-xx-xx, where 'x' is a valid hexadecimal character (0-9, A-F, or a-f). MAC addresses should be separated by at least one blank space.

The MAC address distinguishes individual systems allowing you to set policies for a particular device. To obtain a system's MAC address, you will need the device to connect to the ASA and perform a DAP trace, look for the value of **endpoint.anyconnect.macaddress**. That is the value that you need to enter in the MAC Address Pool field.

Step 8 Click **OK**.

Add a File Endpoint Attribute to a DAP

Before you begin

Before configuring a File endpoint attribute, define the file for which you want to scan in the HostScan/Secure Firewall Posture window.

For HostScan version 4.x, choose **Configuration > Remote Access VPN > Secure Desktop Manager > HostScan** in ASDM. For Secure Firewall Posture version 5.x, choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings** in ASDM.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **File**.

Step 2 Select the appropriate **Exists** or **Does not exist** radio button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Exists/Does not exist buttons) should be present or not.

Step 3 In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID that equates to the file entry for which you want to scan.

The file information is displayed below the Endpoint ID list box.

Step 4 Check the **Last Update** check box and set the operation field to be less than (<) or greater than (>) a certain number of days old. Enter the number of days old in the **days** field.

Step 5 Check the **Checksum** checkbox and set the operation field to be equal to (=) or not equal to (!=) the checksum value of the file you are testing for.

Step 6 Click **Compute CRC32 Checksum** to determine the checksum value of the file you are testing for.

Step 7 Click **OK**.

Add a Device Endpoint Attribute to a DAP

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Device**.

Step 2 Check the **Host Name** checkbox and set the operation field to be equal to (=) or not equal to (!=) the host name of the device you are testing for. Use the computer's host name only, not the fully qualified domain name (FQDN).

Step 3 Check the **MAC address** checkbox and set the operation field to be equal to (=) or not equal to (!=) the MAC address of the network interface card you are testing for. Only one MAC address per entry. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.

Step 4 Check the **BIOS Serial Number** checkbox and set the operation field to be equal to (=) or not equal to (!=) the BIOS serial number value of the device you are testing for. The number format is manufacturer-specific. There is no format requirement.

Step 5 Check the **TCP/UDP Port Number** checkbox and set the operation field to be equal to (=) or not equal to (!=) the TCP or UDP port in listening state that you are testing for.

In the TCP/UDP combo box, choose the kind of port you are testing for: TCP (IPv4), UDP(IPv4), TCP (IPv6), or UDP (IPv6). If you are testing for more than one port, make several individual endpoint attribute rules in the DAP and specify one port in each.

Step 6 Check the **Version of Secure Desktop (CSD)** checkbox and set the operation field to be equal to (=) or not equal to (!=) the version of the HostScan/Secure Firewall Posture image running on the endpoint.

Step 7 Check the **Version of Endpoint Assessment** checkbox and set the operation field to be equal to (=) or not equal to (!=) the version of endpoint assessment (OPSWAT) you are testing for.

Step 8 Click **OK**.

Add a NAC Endpoint Attribute to a DAP

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **NAC**.

Step 2 Check the **Posture Status** checkbox and set the operation field to be equal to (=) or not equal to (!=) the posture token string received by ACS. Enter the posture token string in the Posture Status text box.

Step 3 Click **OK**.

Add an Operating System Endpoint Attribute to a DAP

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Operating System**.

Step 2 Check the **OS Version** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Windows, Mac, or Linux operating system you set in the **OS Version** list box.

Step 3 Check the **OS Update** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Windows, Mac, or Linux service pack for the operating system you enter in the **OS Update** text box.

Step 4 Click **OK**.

Add a Personal Firewall Endpoint Attribute to a DAP

Before you begin

If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Operating System**.

Step 2 Click the appropriate **Installed or Not Installed** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Valud column) are installed or not installed.

Step 3 From the **Vendor** list box, click the name of the personal firewall vendor you are testing for.

Step 4 Check the **Product Description** check box and choose from the list box the vendor's product name you are testing for.

Step 5 Check the **Version** checkbox and set the operation field to equal to (=), not equal (!=), less than (<), greater than (>), less that or equal to (<=), or greater than or equal to (>=) the product version number you choose from the **Version** list box.

If the choice in the **Version** list box has an x, such as 3.x, replace the x with a specific release number, for example, 3.5.

Step 6 Check the **Last Update** check box. Specify the number of days since the last update. You might want to indicate that an update should occur in less than (<) or more than (>) the number of days you enter here.

Step 7 Click **OK.**

Add a Policy Endpoint Attribute to a DAP

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Policy**.

Step 2 Check the **Location** checkbox and set the operation field to be equal to (=) or not equal to (!=) the Cisco Secure Desktop Microsoft Windows location profile. Enter the Cisco Secure Desktop Microsoft Windows location profile string in the **Location** text box.

Step 3 Click **OK**.

Add a Process Endpoint Attribute to a DAP

Before you begin

Before configuring a Process endpoint attribute, define the process for which you want to scan in the HostScan/Secure Firewall Posture window for Cisco Secure Desktop.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Process**.

Step 2 Click the appropriate **Exists or Does not exist** button to indicate whether the selected endpoint attribute and its accompanying qualifiers (fields below the Exists and Does not exist buttons) should be present or not.

Step 3 In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID for which you want to scan.

The endpoint ID process information is displayed below the list box.

Step 4 Click **OK**.

Add a Registry Endpoint Attribute to a DAP

Scanning for registry endpoint attributes applies to Windows operating systems only.

Before you begin

Before configuring a Registry endpoint attribute, define the registry key for which you want to scan in the HostScan/Secure Firewall Posture window.

Procedure

Step 1 In the **Endpoint Attribute Type** list box, choose **Registry**.

Step 2 Click the appropriate **Exists or Does not exist** button to indicate whether the **Registry** endpoint attribute and its accompanying qualifiers (fields below the Exists and Does not exist buttons) should be present or not.

Step 3 In the **Endpoint ID** list box, choose from the drop-down list the endpoint ID that equates to the registry entry for which you want to scan.

The registry information is displayed below the Endpoint ID list box.

Step 4 Check the **Value** checkbox and set the operation field to be equal to (=) or not equal to (!=).

Step 5 In the first **Value** list box, identify the registry key as a dword or a string.

Step 6 In the second Value operation list box, enter the value of the registry key you are scanning for.

Step 7 If you want to disregard the case of the registry entry when scanning, click the checkbox. If you want the search to be case-sensitive, do not check the check box.

Step 8 Click **OK**.

Add Multiple Certificate Authentication Attributes to DAP

You can index each certificate so that any of the received certificates can be referenced by the configured rules. Based on these certificate fields, you can configure DAP rules to allow or disallow connection attempts.

Procedure

Step 1 Browse to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add Endpoint Attribute**.

Step 2 Choose **Multiple Certificate Authentication** as the Endpoint Attribute Type in the drop-down menu.

Step 3 Configure one or all of the following, depending on what your preference is:

- Subject Name
- Issuer Name
- Subject Alternate Name
- Serial Number

Step 4 Leave the Certificate Store at the default of None to allow certificates from either store or choose which to allow, only user or only machine. If you choose User or Machine, you must enter the store that the certificate came from. This information is sent by the client in the protocol.

DAP and Antimalware and Personal Firewall Programs

The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Prelogin Assessment and HostScan/Secure Firewall Posture return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to choose a DAP record that matches the values of those attributes.

Most, but not all, antimalware and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. HostScan/Secure Firewall Posture checks to see if an endpoint has a program installed, and if it is memory-resident as follows:

- If the installed program does not support active scan, HostScan/Secure Firewall Posture reports the presence of the software. The DAP system selects DAP records that specify the program.
- If the installed program does support active scan, and active scan is enabled for the program, HostScan/Secure Firewall Posture reports the presence of the software. Again the security appliance selects DAP records that specify the program.
- If the installed program does support active scan and active scan is disabled for the program, HostScan/Secure Firewall Posture ignores the presence of the software. The security appliance does not choose DAP records that specify the program. Further, the output of the **debug trace** command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.



Note If upgrading from HostScan 4.3.x to HostScan 4.6.x or greater, you must migrate any existing AV/AS/FW endpoint attributes to the corresponding replacement AM/FW endpoint attributes before you upgrade. See the AnyConnect HostScan 4.3.x to 4.6.x Migration Guide for a full upgrade & migration procedure.

Endpoint Attribute Definitions

The following endpoint selection attributes are available for DAP use.The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, used in the Advanced area in Dynamic Access Policy Selection Criteria pane. The *label* variable identifies the application, filename, process, or registry entry.

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Antimalware	endpoint.am["*label*"].exists	Host ScanSecure Firewall Posture	true	—	Antimalware program exists
	endpoint.am["*label*"].version		string	32	Version
	endpoint.am["*label*"].description		string	128	Antimalware description
	endpoint.am["*label*"].lastupdate		integer	—	Seconds since update of antimalware definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Personal firewall	endpoint.pfw["*label*"].exists	Host Scan/Secure Firewall Posture	true	—	The personal firewall exists
	endpoint.pfw["*label*"].version		string	string	Version
	endpoint.pfw["*label*"].description		string	128	Personal firewall description
AnyConnect (Does not require Host Scan/Secure Firewall Posture)	endpoint.anyconnect.clientversion	Endpoint	version	—	AnyConnect Client version
	endpoint.anyconnect.platform		string	—	Operating system on which the AnyConnect Client is installed
	endpoint.anyconnect.platformversion		version	64	Version of operating system on which the AnyConnect Client is installed
	endpoint.anyconnect.devicetype		string	64	Mobile device type on which the AnyConnect Client is installed
	endpoint.anyconnect.deviceuniqueid			64	Unique ID of mobile device on which the AnyConnect Client is installed
	endpoint.anyconnect.macaddress		string	—	MAC Address of device on which the AnyConnect Client is installed Must be in the format xx-xx-xx-xx-xx-xx, where 'x' is a valid hexadecimal character
Application	endpoint.application.clienttype	Application	string	—	Client type: CLIENTLESS ANYCONNECT IPSEC L2TP

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Device	endpoint.device. hostname	Endpoint	string	64	Host Name only. Not FQDN
	endpoint.device.MAC		string	—	Mac Address for a network interface card. Only one Mac address per entry Must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
	endpoint.device.id		string	64	BIOS Serial Number. The number format is manufacturer-specific. There is no format requirement
	endpoint.device.port		string	—	TCP port in listening state You can define a single port per line An integer between 1 and 65535
	endpoint.device. protection_version		string	64	Version of HostScan/Secure Firewall Posture image they are running
	endpoint.device. protection_extension		string	64	Version of Endpoint Assessment (OPSWAT)
File	endpoint.file["*label*"].exists		true	—	The files exists
	endpoint.file[“label”]. endpointid				
	endpoint.file["*label*"]. lastmodified		integer	—	Seconds since file was last modified
	endpoint.file["*label*"]. crc.32		integer	—	CRC32 hash of the file
NAC	endpoint.nac.status	NAC	string	—	User defined status string

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Operating System	endpoint.os.version		string	32	Operating system
	endpoint.os.servicepack		integer	—	Service pack for Windows
Policy	endpoint.policy.location		string	64	
Process	endpoint.process["*label*"].exists		true	—	The process exists
	endpoint.process["*label*"].path		string	255	Full path of the process
Registry	endpoint.registry["*label*"].type		*dword string*	—	dword
	endpoint.registry["*label*"].value		string	255	Value of the registry entry
VLAN	endoint.vlan.type	CNA	string	—	VLAN type: ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

Create Additional DAP Selection Criteria in DAP Using LUA

This section provides information about constructing logical expressions for AAA or endpoint attributes. Be aware that doing so requires sophisticated knowledge of LUA. You can find detailed LUA programming information at http://www.lua.org/manual/5.1/manual.html.

In the Advanced field you enter free-form LUA text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP policy file, and the ASA processes it, discarding any expressions it cannot parse.

This option is useful for adding selection criteria other than what is possible in the AAA and endpoint attribute areas above. For example, while you can configure the ASA to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to create appropriate logical expressions in LUA and enter them here.

The following sections provide detailed explanations of creating LUA EVAL expressions, as well as examples.

- Syntax for Creating LUA EVAL Expressions, on page 181
- Examples of DAP EVAL Expressions, on page 184
- Additional LUA Functions, on page 182

Syntax for Creating LUA EVAL Expressions

Note If you must use Advanced mode, we recommend that you use EVAL expressions whenever possible for reasons of clarity, which makes verifying the program straightforward.

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA attribute or an attribute returned from Cisco Secure Desktop, see Endpoint Attribute Definitions, on page 177 for attribute definitions	
<comparison>	One of the following strings (quotation marks required)	
	“EQ”	equal
	“NE”	not equal
	“LT”	less than
	“GT”	greater than
	“LE”	less than or equal
	“GE”	greater than or equal
<value>	A string in quotation marks that contains the value to compare the attribute against	
<type>	One of the following strings (quotation marks required)	
	“string”	case-sensitive string comparison
	“”	case-insensitive string comparison
	“integer”	number comparison, converts string values to numbers
	“hex”	number comparison using hexadecimal values, converts hex string to hex numbers
	“version”	compares versions of the form X.Y.Z. where X, Y, and Z are numbers

LUA Procedures for HostScan 4.6 (and Later) and Secure Firewall Posture Version 5

LUA Script for 'ANY' Antimalware (endpoint.am) with Last Update

Use the following LUA script to check for 'ANY' antimalware product/vendor (endpoint.am). Modifications may apply to accommodate a different Last Update interval. The following example shows how a Last Update must have been performed in <30 days (noted as 2592000 seconds).

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
             return true
         end
  end
  return false
end)()
```

LUA Script for 'ANY' Personal Firewall

Use the following LUA script to check for 'ANY' firewall product/vendor (endpoint.pfw):

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

Additional LUA Functions

When working with dynamic access policies, you might need additional flexibility of match criteria. For example, you might want to apply a different DAP based on the following:

- CheckAndMsg is a LUA function that you can configure DAP to call. It generates a user message based on a condition.
- Organizational Unit (OU) or other level of the hierarchy for the user object.
- Group names that follow a naming convention with many possible matches might require the ability to use a wildcard.

You can accomplish this flexibility by creating a LUA logical expression in the Advanced section of the DAP pane in ASDM.

The DAP CheckAndMsg Function

The ASA displays the message to the user only when the DAP record containing the LUA CheckAndMsg function is selected and results in a connection termination.

The syntax of the CheckAndMsg function follows:

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

Be aware of the following when creating CheckAndMsg functions:

- CheckAndMsg returns the value passed in as its first argument.
- Use the EVAL function as the first argument if you do not want to use string comparison. For example:

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg returns the result of the EVAL function, and the security appliance uses it to determine whether to choose the DAP record. If the record is selected and results in termination, the security appliance displays the appropriate message.

OU-Based Match Example

DAP can use many attributes returned from an LDAP server in a logical expression. See the DAP trace section for example output of this, or run a debug dap trace.

The LDAP server returns the user Distinguished Name (DN). This implicitly identifies where in the directory the user object is located. For example, if the user DN is CN=Example User, OU=Admins, dc=cisco, dc=com, this user is located in OU=Admins,dc=cisco,dc=com. If all administrators are in this OU, or any container below this level, you can use a logical expression to match this criteria as follows:

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

In this example, the string.find function allows for a regular expression. Use the $ at the end of the string to anchor this string to the end of the distinguishedName field.

Group Membership Example

You can create a basic logical expression for pattern matching of AD group membership. Because users can be members of multiple groups, DAP parses the response from the LDAP server into separate entries in a table. You need an advanced function to accomplish the following:

- Compare the memberOf field as a string (in the event the user belongs to only one group).
- Iterate through each returned memberOf field if the returned data is of type "table."

The function we have written and tested for this purpose is shown below. In this example, if a user is a member of any group ending with "-stu," they match this DAP.

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
```

```
   return false
end)()
```

Deny Access Example

You can use the following function to deny access in the absence of an antimalware program. Use it with a DAP that has Action set to terminate.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

If a user lacking an antimalware program attempts to log in, DAP displays the following message:

```
Please install antimalware software before connecting.
```

Multiple Certificate Authentication Example

You can definite a wildcard issuer CN with Multiple Certificate Authentication in DAP rules.

If you have configured two certificates issued to two different machines by two different certificate authorities (for example abc.cisco.com and xyz.cisco.com), then the DAP rule must have a condition for multiple certificate authentication where the issuer CN is be *.cisco.com or cisco.com.

You can use the following function to define a DAP rule for certificate with wildcard issuer_cn cisco.com for user and machine certificates:

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

Examples of DAP EVAL Expressions

Study these examples for help in creating logical expressions in LUA:

Description	Example
Endpoint LUA checks for Windows 10	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`

Description	Example
Endpoint LUA checks for a match on CLIENTLESS OR CVC client types.	`(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))`
Endpoint LUA checks if a single Antimalware program Symantec Enterprise Protection is installed on the user PC, displays a message if it is not.	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
Endpoint LUA checks for McAfee Endpoint Protection versions 10 to 10.5.3 and versions above 10.6.	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
Endpoint LUA checks if McAfee Antimalware definitions have been updated within the last 10 days(864000 sec) and displays a message if an update is needed.	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
Check for a specific hotfix after debug dap trace returns: `endpoint.os.windows.hotfix["KB923414"] = "true";`	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

Check for Antimalware Programs and Provide Messages

You can configure messages so that the end users are aware of and able to fix problems with their antimalware software. If access is allowed, the ASA displays all messages generated in the process of DAP evaluation on the portal page. If access is denied, the ASA collects all messages for the DAP that caused the "terminate" condition and displays them in the browser on the logon page.

The following example shows how to use this feature to check on the status of Symantec Endpoint Protection.

1. Copy and paste the following LUA expression into the Advanced field of the Add/Edit Dynamic Access Policy pane (click the double arrow on the far right to expand the field).

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
   Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec
    Endpoint Protection is disabled. You must enable before being granted access", nil))
   ```

2. In that same Advanced field, click the **OR** button.
3. In the Access Attributes section below, in the leftmost tab, Action**,** click **Terminate**.
4. Connect from a PC that has Symantec Endpoint Protection installed, but has Symantec Endpoint Protection disabled. The expected result is that the connection is not allowed and that the user will be presented the message "Symantec Endpoint Protection is disabled. You must enable before being granted access."

Check for Antimalware Programs and Definitions Older than 2 Days

This example checks for the presence of the Symantec and McAfee antimalware programs, and whether the virus definitions are older than 2 days (172,800 seconds). If the definitions are older than 2 days, the ASA terminates the session with a message and links for remediation. To accomplish this task, perform the following steps.

1. Copy and paste the following LUA expression into the Advanced field of the Add/Edit Dynamic Access Policy pane:

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
"Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
 before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
"McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
 Virus Definitions before being granted access", nil))
```

2. In that same Advanced field, click **AND**.
3. In the Access Attributes section below, in leftmost tab Action, click **Terminate**.
4. Connect from a PC that has Symantec and McAfee antimalware programs with versions that are older than 2 days.

   The expected result is that the connection is not allowed and that the user is presented a message that the virus definitions are out of date.

Configure DAP Access and Authorization Policy Attributes

Click each of the tabs and configure the contained fields.

Procedure

Step 1 Select the **Action** tab to specify special processing to apply to a specific connection or session.

- Continue—(Default) Click to apply access policy attributes to the session.
- Quarantine—Through the use of quarantine, you can restrict a particular client who already has an established tunnel through a VPN. ASA applies restricted ACLs to a session to form a restricted group, based on the selected DAP record. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation, but restrictions are placed upon the user. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects. This parameter requires an AnyConnect Client release that supports AnyConnect Secure Mobility features.
- Terminate—Click to terminate the session.
- User Message—Enter a text message to display on the portal page when this DAP record is selected. Maximum 490 characters. A user message displays as a yellow orb. When a user logs on, it blinks three times to attract attention, and then it is still. If several DAP records are selected, and each of them has a user message, all of the user messages display.

You can include URLs or other embedded text, which require that you use the correct HTML tags. For example: All contractors read Instructions for the procedure to upgrade your anti-malware software.

Step 2 Select the **Network ACL Filters** tab to configure network ACLs to apply to this DAP record.

An ACL for DAP can contain permit or deny rules, but not both. If an ACL contains both permit and deny rules, the ASA rejects it.

- Network ACL drop-down list—Select already configured network ACLs to add to this DAP record. The ACLs may be any combination of permit and deny rules. This field supports unified ACLs which can define access rules for IPv4 and IPv6 network traffic.
- **Manage**—Click to add, edit, and delete network ACLs.
- **Network ACL list**—Displays the network ACLs for this DAP record.
- **Add**— Click to add the selected network ACL from the drop-down list to the Network ACLs list on the right.
- **Delete**—Click to delete a highlighted network ACL from the Network ACLs list. You cannot delete an ACL from the ASA unless you first delete it from DAP records.

Step 3 Select the **Web-Type ACL Filters (clientless)** tab to configure web-type ACLs to apply to this DAP record. An ACL for DAP can contain only permit or deny rules. If an ACL contains both permit and deny rules, the ASA rejects it.

- **Web-Type ACL** drop-down list—Select already configured web-type ACLs to add to this DAP record. The ACLs may be any combination of permit and deny rules.
- **Manage**—Click to add, edit, and delete web-type ACLs.
- **Web-Type ACL** list—Displays the web-type ACLs for this DAP record.
- **Add**—Click to add the selected web-type ACL from the drop-down list to the Web-Type ACLs list on the right.
- **Delete**—Click to delete a web-type ACL from the Web-Type ACLs list. You cannot delete an ACL from the ASA unless you first delete it from DAP records.

Step 4 Select the **Functions** tab to configure file server entry and browsing, HTTP proxy, and URL entry for the DAP record.

- **File Server Browsing**—Enables or disables CIFS browsing for file servers or shared features.

  Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS. The CIFS browse feature does not support internationalization.
- **File Server Entry**—Lets or prohibits a user from entering file server paths and names on the portal page. When enabled, places the file server entry drawer on the portal page. Users can enter pathnames to Windows files directly. They can download, edit, delete, rename, and move files. They can also add files and folders. Shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.
- **HTTP Proxy**—Affects the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with proper content transformation, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy

modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.

- **URL Entry**—Allows or prevents a user from entering HTTP/HTTPS URLs on the portal page. If this feature is enabled, users can enter web addresses in the URL entry box.

Using SSL VPN does not ensure that communication with every site is secure. SSL VPN ensures the security of data transmission between the remote user PC or workstation and the ASA on the corporate network. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate ASA to the destination web server is not secured.

In a clientless VPN connection, the ASA acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the ASA establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore cannot examine and validate the certificate. The current implementation of SSL VPN does not permit communication with sites that present expired certificates. Neither does the ASA perform trusted CA certificate validation. Therefore, users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To limit Internet access for users, choose Disable for the URL Entry field. This prevents SSL VPN users from surfing the web during a clientless VPN connection.

- **Unchanged**—(default) Click to use values from the group policy that applies to this session.
- **Enable/Disable**—Click to enable or disable the feature.
- **Auto-start**—Click to enable HTTP proxy and to have the DAP record automatically start the applets associated with these features.

Step 5 Select the **Port Forwarding Lists** tab to configure port forwarding lists for user sessions.

Port Forwarding provides access for remote users in the group to client/server applications that communicate over known, fixed TCP/IP ports. Remote users can use client applications that are installed on their local PC and securely access a remote server that supports that application. Cisco has tested the following applications: Windows Terminal Services, Telnet, Secure FTP (FTP over SSH), Perforce, Outlook Express, and Lotus Notes. Other TCP-based applications may also work, but Cisco has not tested them.

Note
Port Forwarding does not work with some SSL/TLS versions.

Caution
Make sure Sun Microsystems Java Runtime Environment (JRE) is installed on the remote computers to support port forwarding (application access) and digital certificates.

- **Port Forwarding**—Select an option for the port forwarding lists that apply to this DAP record. The other attributes in this field are enabled only when you set Port Forwarding to Enable or Auto-start.
- **Unchanged**—Click to remove the attributes from the running configuration.
- **Enable/Disable**—Click to enable or disable port forwarding.
- **Auto-start**—Click to enable port forwarding, and to have the DAP record automatically start the port forwarding applets associated with its port forwarding lists.

- **Port Forwarding List** drop-down list—Select already configured port forwarding lists to add to the DAP record.
- **New...**—Click to configure new port forwarding lists.
- **Port Forwarding Lists** (unlabeled)—Displays the port forwarding lists for the DAP record.
- **Add**—Click to add the selected port forwarding list from the drop-down list to the Port Forwarding list on the right.
- **Delete**—Click to delete selected port forwarding list from the Port Forwarding list. You cannot delete a port forwarding list from the ASA unless you first delete it from DAP records.

Step 6 Select the **Bookmarks** tab to configure bookmarks for certain user session URLs.

- **Enable bookmarks**—Click to enable. When unchecked, no bookmarks display in the portal page for the connection.
- **Bookmark** drop-down list—Choose already configured bookmarks to add to the DAP record.
- **Manage...**—Click to add, import, export, and delete bookmarks.
- **Bookmarks (unlabeled)**—Displays the URL lists for the DAP record.
- **Add>>**—Click to add the selected bookmark from the drop-down list to the URL area on the right.
- **Delete**—Click to delete the selected bookmark from the URL list area. You cannot delete a bookmark from the ASA unless you first delete it from DAP records.

Step 7 Select the **Access Method** tab to configure the type of remote access permitted.

- **Unchanged**—Continue with the current remote access method.
- **AnyConnect Client**—Connect using the AnyConnect VPN module of Cisco Secure Client

  .
- **Web-Portal**—Connect with clientless VPN.
- **Both-default-Web-Portal**—Connect via either clientless or the AnyConnect Client, with a default of clientless.
- **Both-default-AnyConnect Client**—Connect via either clientless or the AnyConnect Client, with a default of AnyConnect Client.

Step 8 Select the **AnyConnect Client** tab to choose the status of the Always-on VPN flag.

- Always-On VPN for AnyConnect Client—Determine if the always-on VPN flag setting in the AnyConnect Client service profile is unchanged, disabled, or if the AnyConnect Client profile setting should be used.

  This parameter requires a release of the Cisco Web Security appliance that provides Secure Mobility Solution licensing support for the AnyConnect VPN module of Cisco Secure Client. It also requires an AnyConnect Client release that supports “Secure Mobility Solution” features. Refer to the *Cisco AnyConnect VPN Client Administrator Guide* for additional information.

Step 9 Select the AnyConnect Client **Custom Attributes** tab to view and associate previously defined custom attributes to this policy. You can also define custom attributes and then associate them with this policy.

Custom attributes are sent to and used by the AnyConnect Client to configure features such as Deferred Upgrade. A custom attribute has a type and a named value. The type of the attribute is defined first, then one or more named values of this type can be defined. For details about the specific custom attributes to configure for a feature, see the *Cisco Secure Client Administrator Guide* for the AnyConnect Client release you are using.

Custom attributes can be predefined in **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** AnyConnect Client **Custom Attributes** and **AnyConnect Client Custom Attribute Names**. Predefined custom attributes are used by both Dynamic Access Policies and Group Policies.

Configure SAML Authorization Using DAP

You can configure SAML authorization and group policy selections using DAP, without having to rely on an external server (RADIUS or LDAP) to retrieve authorization attributes.

The SAML Identity Provider can be configured to send authorization attributes in addition to the authentication assertions. The SAML Service Provider component in ASA interprets the SAML assertions and makes authorization or group policy selections based on the received assertions. The assertion attributes are processed using DAP rules configured by ASDM.

The Group Policy attribute must use the attribute name **cisco_group_policy**. This attribute is not dependent on DAP being configured. However, if a DAP is configured, it can be used as part of the DAP policy.

Group Policy Selection

If an attribute with the name **cisco_group_policy** is received, the corresponding value is used to select the connection group-policy.

When a connection is made, group-policy information can be taken from multiple sources and combined to form an effective group-policy that is applied to the connection.

The following scenarios are possible while combining the group-policy information received:

Group-policy received in SAML authentication, authorization NOT configured

In this scenario, the effective group-policy is determined as follows in order of decreasing priority:

1. Group-policy specified in SAML attribute.
2. Group-policy specified in the tunnel-group.
3. Default group-policy.

Group-policy received in SAML authentication, authorization configured

In this scenario, the effective group-policy is determined as follows in order of decreasing priority:

1. Group-policy specified in authorization attributes.
2. User group-policy: use value returned from authorization server if present.
3. User group-policy: use the value returned in SAML attribute.
4. Group-policy specified in the tunnel-group.
5. Default group-policy.

Procedure

Step 1 In ASDM, select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** .

Step 2 In the AAA attributes selection area, click **Add**.

a) From the **AAA Attribute Type** drop down, select SAML.
b) Specify *memberOf* as the **Attribute ID**.
c) Enter the *memberOf* attribute **Value** or click **Get AD Group** if the AD server groups are configured.

To configure additional AD Server Groups go to **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.

To configure group-policy selection attributes, select the following settings in the same DAP policy or in another DAP policy as required:

- **AAA Attribute Type**: SAML
- **Attribute ID**: cisco_group_policy
- **Value**: Name of the group policy

Step 3 Click **OK**.

Step 4 Click **OK** to save the DAP policy.

Perform a DAP Trace

A DAP trace displays the DAP endpoint attributes for all connected devices.

Procedure

Step 1 Log on to the ASA from an SSH terminal and enter Privileged Exec mode.

In Privileged Exec mode, the ASA prompts: `hostname#`.

Step 2 Enable DAP debugs to display all DAP attributes for the session in the terminal window:

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

Step 3 (Optional) In order to search the output of the DAP trace, send the output of the command to a system log. To learn more about logging on the ASA see *Configure Logging* in the *Cisco ASA Series General Operations ASDM Configuration Guide*.

Examples of DAPs

- Use DAP to Define Network Resources, on page 192
- Use DAP to Apply a WebVPN ACL, on page 193
- Enforce CSD Checks and Apply Policies via DAP, on page 193

Use DAP to Define Network Resources

This example shows how to configure dynamic access policies as a method of defining network resources for a user or group. The DAP policy named Trusted_VPN_Access permits clientless and AnyConnect VPN module of Cisco Secure Client access. The policy named Untrusted_VPN_Access permits only clientless VPN access.

Procedure

Step 1 In ASDM, go to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** > **Endpoint**.

Step 2 Configure the following attributes for each policy:

Attribute	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	Trusted	Untrusted
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	Untrusted
LDAP memberOf	Engineering, Managers	Vendors
ACL		Web-Type ACL
Access	**AnyConnect Client** *and* **Web Portal**	**Web Portal**

Use DAP to Apply a WebVPN ACL

DAP can directly enforce a subset of access policy attributes including Network ACLs (for IPsec and AnyConnect Client), URL lists, and Functions. It cannot directly enforce, for example, a banner or the split tunnel list, which the group policy enforces. The Access Policy Attributes tabs in the Add/Edit Dynamic Access Policy pane provide a complete menu of the attributes DAP directly enforces.

Active Directory/LDAP stores user group policy membership as the "memberOf" attribute in the user entry. Define a DAP such that for a user in AD group (memberOf) = Engineering the ASA applies a configured Web-Type ACL.

Procedure

Step 1 In ASDM got to the Add AAA attributes pane, **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** > **AAA Attributes section** > **Add AAA Attribute**.

Step 2 For the AAA Attribute type, use the drop-down list to choose **LDAP**.

Step 3 In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.

Step 4 In the Value field, use the drop-down list to choose =, and in the adjacent field enter Engineering.

Step 5 In the Access Policy Attributes area of the pane, click the Web-Type ACL Filters tab.

Step 6 Use the Web-Type ACL drop-down list to choose the ACL you want to apply to users in the AD group (memberOf) = Engineering.

Enforce CSD Checks and Apply Policies via DAP

This example creates a DAP that checks that a user belongs to two specific AD/LDAP groups (Engineering and Employees) and a specific ASA tunnel group. It then applies an ACL to the user.

The ACLs that DAP applies control access to the resources. They override any ACLS defined the group policy on the ASA. In addition, the ASA applied the regular AAA group policy inheritance rules and attributes for those that DAP does not define or control, examples being split tunneling lists, banner, and DNS.

Procedure

Step 1 In ASDM got to the Add AAA attributes pane, **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** > **AAA Attributes section** > **Add AAA Attribute**.

Step 2 For the AAA Attribute type, use the drop-down list to choose LDAP.

Step 3 In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.

Step 4 In the Value field, use the drop-down list to choose =, and in the adjacent field enter Engineering.

Step 5 In the Attribute ID field, enter memberOf, exactly as you see it here. Case is important.

Step 6 In the Value field, use the drop-down list to choose =, and in the adjacent field enter Employees.

Step 7 For the AAA attribute type, use the drop-down list to choose Cisco.

Step 8 Check the Tunnel group box, use the drop-down list to choose =, and in the adjacent drop-down list choose the appropriate tunnel group (connection policy).

Step 9 In the Network ACL Filters tab of the Access Policy Attributes area, choose the ACLs to apply to users who meet the DAP criteria defined in the previous steps.

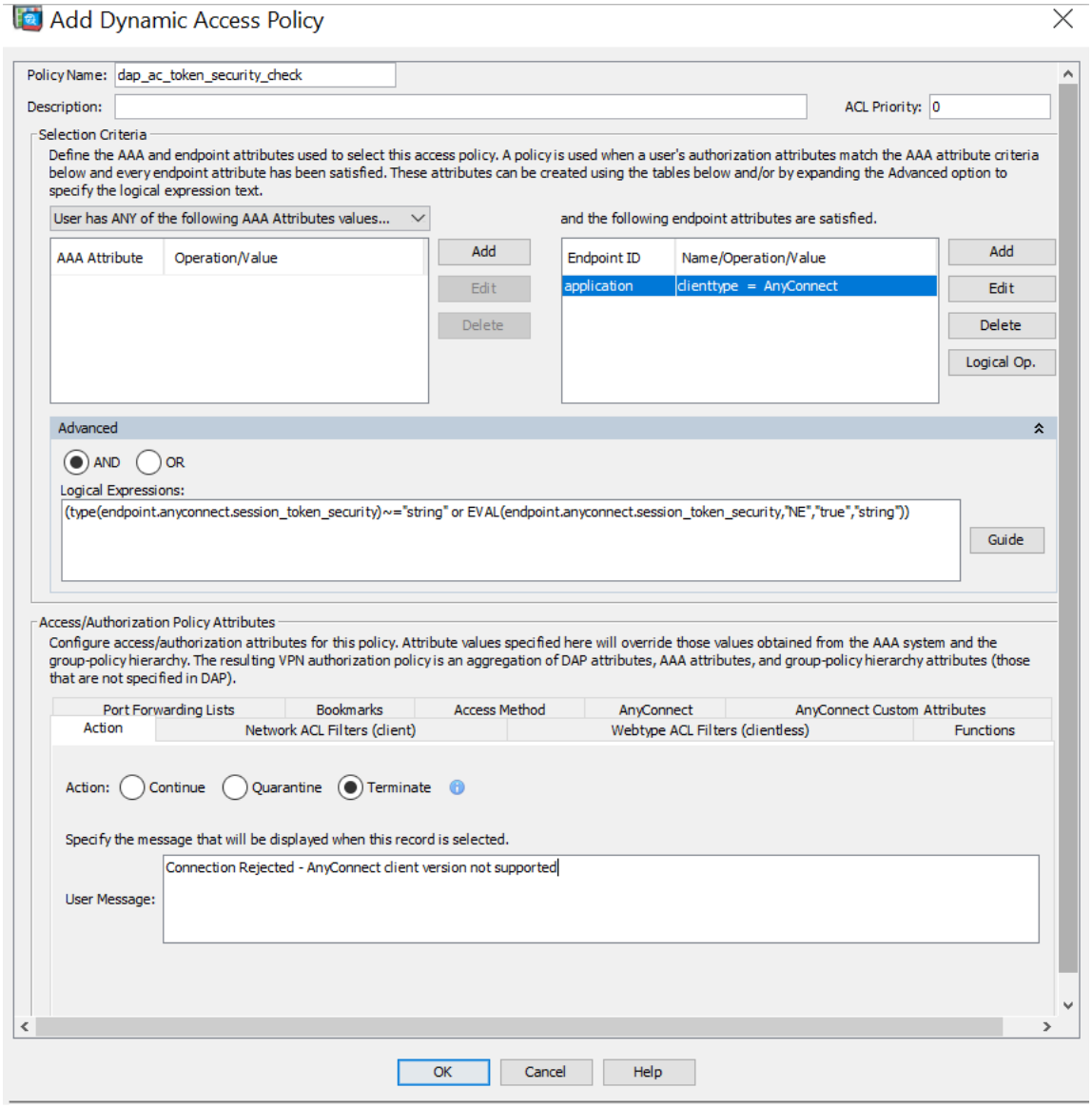
Use DAP to Check Session Token Security

When the ASA authenticates a VPN connection request from the AnyConnect Client, the ASA returns a session token to the client. Starting with AnyConnect 4.9 (MR1), the ASA and AnyConnect Client support a mechanism that provides enhanced security for the session token. You must configure a DAP to ensure that the AnyConnect Client supports session token security.

Use the this DAP with endpoint attribute settings, and LUA script to reject connection attempts from AnyConnect Client versions that do not support token security.

Procedure

Step 1 In ASDM, select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** .



Step 2 In the endpoint attributes selection area, click **Add**.

a) From the **Endpoint Attribute Type** drop down, select Application.

b) For the **Client Type**, select the equals (=) operator and then select AnyConnect Client from the drop-down.

c) Click **OK**.

Step 3 Configure the **Advanced** selection criteria:

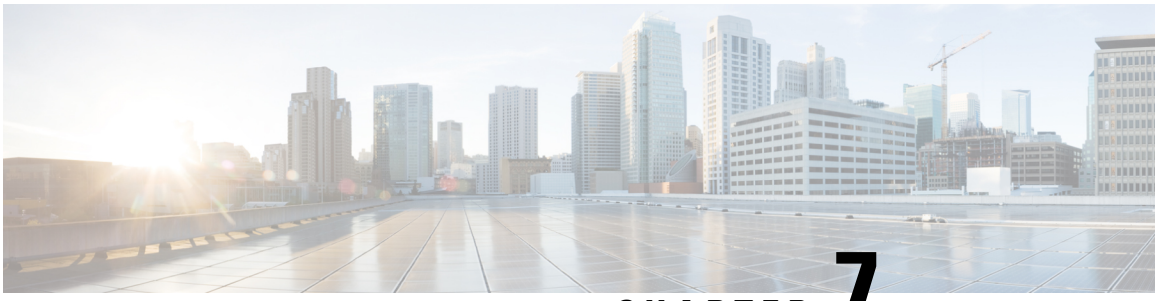
a) Select the **AND** operator.

b) Add the **Logical Expression**

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

Step 4 In the **Action** area, select **Terminate**.

Step 5 Add an optional User Message and click **OK**.



CHAPTER 7

Email Proxy

Email proxies extend remote email capability to users of Clientless SSL VPN. When users attempt an email session via email proxy, the email client establishes a tunnel using the SSL protocol.

The email proxy protocols are as follows:

POP3S

POP3S is one of the email proxies Clientless SSL VPN supports. By default the Security Appliance listens to port 995, and connections are automatically allowed to port 995 or to the configured port. The POP3 proxy allows only SSL connections on that port. After the SSL tunnel is established, the POP3 protocol starts, and then authentication occurs. POP3S is for a receiving email.

IMAP4S

IMAP4S is one of the email proxies Clientless SSL VPN supports. By default the Security Appliance listens to port 993, and connections are automatically allowed to port 993 or to the configured port. The IMAP4 proxy allows only SSL connections on that port. After the SSL tunnel is established, the IMAP4 protocol starts, and then authentication occurs. IMAP4S is for receiving email.

SMTPS

SMTPS is one of the email proxies Clientless SSL VPN supports. By default, the Security Appliance listens to port 988, and connections automatically are allowed to port 988 or to the configured port. The SMTPS proxy allows only SSL connections on that port. After the SSL tunnel establishes, the SMTPS protocol starts, and then authentication occurs. SMTPS is for sending email.

- Configure Email Proxy, on page 198
- Set AAA Server Groups, on page 198
- Identify Interfaces for Email Proxy, on page 199
- Configure Authentication for Email Proxy, on page 200
- Identify Proxy Servers, on page 201
- Configure Delimiters, on page 202

Configure Email Proxy

Requirements for Email Proxy

- Users who access email from both local and remote locations via email proxy require separate email accounts on their email program for local and remote access.
- Email proxy sessions require that the user authenticate.

Set AAA Server Groups

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **AAA.**

Step 2 Choose the appropriate tab (POP3S , IMAP4S , or SMTPS) to associate AAA server groups and configure the default group policy for those sessions.

- AAA server groups—Click to go to the AAA Server Groups panel (Configuration > Features > Properties > AAA Setup > AAA Server Groups), where you can add or edit AAA server groups.
- group policies—Click to go to the Group Policy panel (Configuration > Features > VPN > General > Group Policy), where you can add or edit group policies.
- Authentication Server Group—Select the authentication server group for user authentication. The default is to have no authentication servers configured. If you have AAA set as the authentication method (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel), you must configure an AAA server and choose it here, or authentication always fails.
- Authorization Server Group—Select the authorization server group for user authorization. The default is to have no authorization servers configured.
- Accounting Server Group—Select the accounting server group for user accounting. The default is to have no accounting servers configured.
- Default Group Policy—Select the group policy to apply to users when AAA does not return a CLASSID attribute. The length must be between 4 and 15 alphanumeric characters. If you do not specify a default group policy, and there is no CLASSID, the ASA cannot establish the session.
- Authorization Settings—Set values for usernames that the ASA recognizes for authorization. This applies to users that authenticate with digital certificates and require LDAP or RADIUS authorization.
  - Use the entire DN as the username—Select to use the Distinguished Name for authorization.
  - Specify individual DN fields as the username—Select to specify specific DN fields for user authorization.

    You can choose two DN fields, primary and secondary. For example, if you choose EA, users authenticate according to their email address. Then a user with the Common Name (CN) John Doe and an email address of johndoe@cisco.com cannot authenticate as John Doe or as johndoe. He

must authenticate as johndoe@cisco.com. If you choose EA and O, John Doe must authenticate as johndoe@cisco.com and Cisco Systems, Inc.

- Primary DN Field—Select the primary DN field thar you want to configure for authorization. The default is CN. Options include the following:

DN Field	Definition
Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
DN Qualifier (DNQ)	A specific DN attribute.
E-mail Address (EA)	The email address of the person, system or entity that owns the certificate.
Generational Qualifier (GENQ)	A generational qualifier such as Jr., Sr., or III.
Given Name (GN)	The first name of the certificate owner.
Initials (I)	The first letters of each part of the certificate owner's name.
Locality (L)	The city or town where the organization is located.
Name (N)	The name of the certificate owner.
Organization (O)	The name of the company, institution, agency, association, or other entity.
Organizational Unit (OU)	The subgroup within the organization.
Serial Number (SER)	The serial number of the certificate.
Surname (SN)	The family name or last name of the certificate owner.
State/Province (S/P)	The state or province where the organization is located.
Title (T)	The title of the certificate owner, such as Dr.
User ID (UID)	The identification number of the certificate owner.

- Secondary DN Field—(Optional) Select the secondary DN field that you want to configure for authorization. The default is OU. Options include all of those in the preceding table, with the addition of **None**, which you choose if you do not want to include a secondary field.

Identify Interfaces for Email Proxy

The Email Proxy Access screen lets you identify interfaces on which to configure email proxy. You can configure and edit email proxies on individual interfaces, and you can configure and edit email proxies for

one interface and then apply your settings to all interfaces. You cannot configure email proxies for management-only interfaces, or for subinterfaces.

Procedure

Step 1 Browse to **Configuration** > **VPN** > **E-Mail Proxy** > **Access** to show what is enabled for the interfaces.

- Interface—Displays the names of all configured interfaces.
- POP3S Enabled—Shows whether POP3S is enabled for the interface.
- IMAP4s Enabled—Shows whether IMAP4S is enabled for the interface.
- SMTPS Enabled—Shows whether SMTPS is enabled for the interface.

Step 2 Click **Edit** to change the email proxy settings for the highlighted interface.

Configure Authentication for Email Proxy

Configure the authentication methods for each of the email proxy types.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Authentication.**

Step 2 Choose from the multiple methods of authentication:

- AAA—Select to require AAA authentication. This option requires a configured AAA server. The user presents a username, server, and password. Users must present both the VPN username and the email username, separated by the VPN Name Delimiter, only if the usernames are different from each other.
- Certificate—Select to require certificate authentication.

  Note
  Certificate authentication does not work for email proxies in the current ASA software release.

  Certificate authentication requires that users have a certificate that the ASA can validate during SSL negotiation. You can use certificate authentication as the only method of authentication, for SMTPS proxy. Other email proxies require two authentication methods.

  Certificate authentication requires three certificates, all from the same CA:

  - A CA certificate on the ASA.

  - A CA certificate on the client PC.

  - A Web Browser certificate on the client PC, sometimes called a Personal certificate or a Web Browser certificate.
- Piggyback HTTPS—Select to require piggyback authentication.

This authentication scheme requires a user to have already established a Clientless SSL VPN session. The user presents an email username only. No password is required. Users must present both the VPN username and the email username, separated by the VPN Name Delimiter, only if the usernames are different from each other.

IMAP generates a number of sessions that are not limited by the simultaneous user count but do count against the number of simultaneous logins allowed for a username. If the number of IMAP sessions exceeds this maximum and the Clientless SSL VPN connection expires, a user cannot subsequently establish a new connection. There are several solutions:

SMTPS email most often uses piggyback authentication because most SMTP servers do not allow users to log in.

Note
IMAP generates a number of sessions that are not limited by the simultaneous user count but do count against the number of simultaneous logins allowed for a username. If the number of IMAP sessions exceeds this maximum and the Clientless SSL VPN connection expires, a user cannot subsequently establish a new connection. There are several solutions:

- The user can close the IMAP application to clear the sessions with the ASA, and then establish a new Clientless SSL VPN connection.

- The administrator can increase the simultaneous logins for IMAP users (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General).

- Disable HTTPS/Piggyback authentication for email proxy.

- Mailhost—(SMTPS only) Select to require mailhost authentication. This option appears for SMTPS only because POP3S and IMAP4S always perform mailhost authentication. It requires the user's email username, server, and password.

Identify Proxy Servers

This Default Server panel lets you identify proxy servers to the ASA and configure a default server, port, and non-authenticated session limit for email proxies.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Default Servers.**

Step 2 Configure the following fields:

- Name or IP Address—Type the DNS name or IP address for the default email proxy server.
- Port—Type the port number on which the ASA listens for email proxy traffic. Connections are automatically allowed to the configured port. The email proxy allows only SSL connections on this port. After the SSL tunnel is established, the email proxy starts, and then authentication occurs.

  The defaults are as follows:

  - 995 (for POP3S)

- 993 (for IMAP4S)
- 988 (for SMTPS)

- Enable non-authenticated session limit—Select to restrict the number of non-authenticated email proxy sessions. Lets you set a limit for session in the process of authenticating, thereby preventing DOS attacks. When a new session exceeds the set limit, the ASA terminates the oldest non-authenticating connection. If no non-authenticating connection exist, the oldest authenticating connection is terminated without terminating the authenticated sessions.

Email proxy connections have three states:

- Unauthenticated—State of new email connections.
- Authenticating—State when the connection presents a username.
- Authenticated—State when the ASA authenticates the connection.

Configure Delimiters

This panel configures username/password delimiters and server delimiters for email proxy authentication.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Delimiters.**

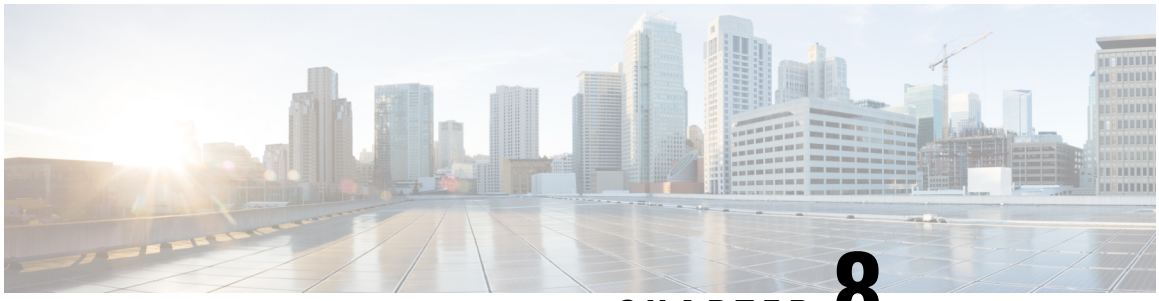
Step 2 Configure the following fields:

- Username/Password Delimiter—Select a delimiter to separate the VPN username from the email username. Users need both usernames when using AAA authentication for email proxy, and the VPN username and email username are different. When they log in to an email proxy session, users enter both usernames, separated by the delimiter you configure here, and also the email server name.

  Note
  Passwords for Clientless SSL VPN email proxy users cannot contain characters that are used as delimiters.

- Server Delimiter—Select a delimiter to separate the username from the name of the email server. It must be different from the VPN Name Delimiter. Users enter both their username and server in the username field when they log in to an email proxy session.

  For example, using : as the VPN Name Delimiter and @ as the Server Delimiter, when logging in to an email program via email proxy, users would enter their username in the following format: vpn_username:e-mail_username@server.



CHAPTER 8

Monitor VPN

- Monitor VPN Connection Graphs, on page 203
- Monitor VPN Statistics, on page 203

Monitor VPN Connection Graphs

See the following screens for showing VPN connection data in graphical or tabular form for the ASA.

Monitor IPsec Tunnels

Monitoring> VPN> VPN Connection Graphs> IPSec Tunnels

For specifying graphs and tables of the IPsec tunnel types that you want to view or to prepare for export or print.

Monitor Sessions

Monitoring> VPN> VPN Connection Graphs> Sessions

For specifying graphs and table of the VPN session types that you want to view or to prepare for export or print.

Monitor VPN Statistics

See the following screens for showing detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. The contents of the statistical tables depend on the type of connection you choose. The detail tables show all the relevant parameters for each session.

Monitor Session Window

Monitoring> VPN> VPN Statistics> Sessions

For viewing VPN session statistics for the ASA. The contents of the second table in this pane depend on the selection in the Filter By list.

Note An administrator can keep track of the number of users in the inactive state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in. You can also access these statistics using the **show vpn-sessiondb** CLI command (refer to the appropriate release of the Cisco ASA Command Reference Guide.

- All Remote Access

  Indicates that the values in this table relate to remote access (IPsec software and hardware clients) traffic.

- Username/Connection Profile—Shows the username or login name and the connection profile (tunnel group) for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.
- Group Policy Connection Profile—Displays the tunnel group policy connection profile for the session.
- Assigned IP Address/Public IP Address—Shows the private ("assigned") IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network. Also shows the Public IP address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
- Ping—Sends an ICMP ping (Packet Internet Groper) packet to test network connectivity. Specifically, the ASA sends an ICMP Echo Request message to a selected host. If the host is reachable, it returns an Echo Reply message, and the ASA displays a Success message with the name of the tested host, as well as the elapsed time between when the request was sent and the response received. If the system is unreachable for any reason, (for example: host down, ICMP not running on host, route not configured, intermediate router down, or network down or congested), the ASA displays an Error screen with the name of the tested host.
- Logout By—Chooses a criterion to use to filter the sessions to be logged out. If you choose any but --All Sessions--, the box to the right of the Logout By list becomes active. If you choose the value Protocol for Logout By, the box becomes a list, from which you can choose a protocol type to use as the logout filter. The default value of this list is IPsec. For all choices other than Protocol, you must supply an appropriate value in this column.

Monitor Active VPN Sessions

Monitoring > VPN > VPN Statistics > Sessions

For viewing AnyConnect Client sessions sorted by username, IP address, address type, or public address.

Monitor VPN Session Details

Monitoring> VPN> VPN Statistics> Sessions> Details

For viewing configuration settings, statistics, and state information about the selected session.

- NAC Result and Posture Token

The ASDM displays values in this column only if you configured Network Admission Control on the ASA.

- Accepted—The ACS successfully validated the posture of the remote host.

- Rejected—The ACS could not successfully validate the posture of the remote host.
- Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the ASA.
- Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.
- Hold-off—The ASA lost EAPoUDP communication with the remote host after successful posture validation.
- N/A—NAC is disabled for the remote host according to the VPN NAC group policy.
- Unknown—Posture validation is in progress.

The posture token is an informational text string which is configurable on the Access Control Server. The ACS downloads the posture token to the ASA for informational purposes to aid in system monitoring, reporting, debugging, and logging. The typical posture token that follows the NAC result is as follows: Healthy, Checkup, Quarantine, Infected, or Unknown.

The Details tab in the Session Details pane displays the following columns:

- ID—Unique ID dynamically assigned to the session. The ID serves as the ASA index to the session. It uses this index to maintain and display information about the session.
- Type—Type of session: IKE, IPsec, or NAC.
- Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port—Addresses and ports assigned to both the actual (Local) peer and those assigned to this peer for the purpose of external routing.
- Encryption—Data encryption algorithm this session is using, if any.
- Assigned IP Address and Public IP Address—Shows the private IP address assigned to the remote peer for this session. Also called the inner or virtual IP address, the assigned IP address lets the remote peer appear to be on the private network. The second field shows the public IP address of the remote computer for this session. Also called the outer IP address, the public IP address is typically assigned to the remote computer by the ISP. It lets the remote computer function as a host on the public network.
- Other—Miscellaneous attributes associated with the session.

The following attributes apply to IKE sessions, IPsec sessions, and NAC sessions:

- Revalidation Time Interval— Interval in seconds required between each successful posture validation.
- Time Until Next Revalidation—0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
- Status Query Time Interval—Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the ASA to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
- EAPoUDP Session Age—Number of seconds since the last successful posture validation.
- Hold-Off Time Remaining—0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.

- Posture Token—Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the ASA for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
- Redirect URL—Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the ASA. The Redirect URL is an optional part of the access policy payload. The ASA redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the ASA does not redirect HTTP and HTTPS requests from the remote host.

  Redirect URLs remain in force until either the IPsec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.

  More—Press this button to revalidate or initialize the session or tunnel group.

The ACL tab displays the ACL containing the ACEs that matched the session.

Monitor Cluster Loads

Monitoring> VPN> VPN Statistics> Cluster Loads

For viewing the current traffic load distribution among the servers in a VPN load-balancing cluster. If the server is not part of a cluster, you receive an information message saying that this server does not participate in a VPN load-balancing cluster.

Monitor Crypto Statistics

Monitoring > VPN> VPN Statistics> Crypto Statistics

For viewing the crypto statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one crypto statistic.

Monitor Compression Statistics

Monitoring> VPN> VPN Statistics> Compression Statistics

For viewing the compression statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one compression statistic.

Monitor Encryption Statistics

Monitoring> VPN> VPN Statistics> Encryption Statistics

For viewing the data encryption algorithms used by currently active user and administrator sessions on the ASA. Each row in the table represents one encryption algorithm type.

Monitor Global IKE/IPsec Statistics

Monitoring> VPN> VPN Statistics> Global IKE/IPSec Statistics

For viewing the global IKE/IPsec statistics for currently active user and administrator sessions on the ASA. Each row in the table represents one global statistic.

Monitor NAC Session Summary

For viewing the active and cumulative Network Admission Control sessions.

- Active NAC Sessions—General statistics about remote peers that are subject to posture validation.
- Cumulative NAC Sessions—General statistics about remote peers that are or have been subject to posture validation.
- Accepted—Number of peers that passed posture validation and have been granted an access policy by an Access Control Server.
- Rejected—Number of peers that failed posture validation or were not granted an access policy by an Access Control Server.
- Exempted—Number of peers that are not subject to posture validation because they match an entry in the Posture Validation Exception list configured on the ASA.
- Non-responsive—Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the ASA configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the ASA for these peers. Otherwise, the ASA assigns the NAC default policy.
- Hold-off—Number of peers for which the ASA lost EAPoUDP communications after a successful posture validation. The NAC Hold Timer attribute (Configuration > VPN > NAC) determines the delay between this type of event and the next posture validation attempt.
- N/A—Number of peers for which NAC is disabled according to the VPN NAC group policy.
- Revalidate All—Click if the posture of the peers or the assigned access policies (that is, the downloaded ACLs), have changed. Clicking this button initiates new, unconditional posture validations of all NAC sessions managed by the ASA. The posture validation and assigned access policy that were in effect for each session before you clicked this button remain in effect until the new posture validation succeeds or fails. Clicking this button does not affect sessions that are exempt from posture validation.
- Initialize All—Click if the posture of the peers or the assigned access policies (that is, the downloaded ACLs) have changed, and you want to clear the resources assigned to the sessions. Clicking this button purges the EAPoUDP associations and assigned access policies used for posture validations of all NAC sessions managed by the ASA, and initiates new, unconditional posture validations. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. Clicking this button does not affect sessions that are exempt from posture validation.

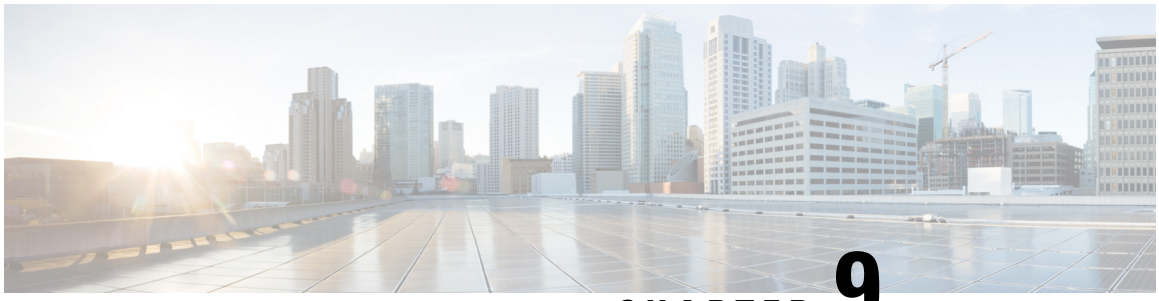
Monitor Protocol Statistics

Monitoring> VPN> VPN Statistics> Protocol Statistics

For viewing the protocols used by currently active user and administrator sessions on the ASA. Each row in the table represents one protocol type.

Monitor VLAN Mapping Sessions

For viewing the number of sessions assigned to an egress VLAN, as determined by the value of the Restrict Access to VLAN parameter of each group policy in use. The ASA forwards all traffic to the specified VLAN.



CHAPTER 9

SSL Settings

• SSL Settings, on page 209

SSL Settings

Configure the SSL Settings at either of the following locations:

- **Configuration > Device Management > Advanced > SSL Settings**
- **Configuration > Remote Access VPN > Advanced > SSL Settings**

The ASA uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for ASDM, Clientless SSL VPN, VPN, and browser-based sessions. In addition, DTLS is used for Secure Client connections. The SSL Settings pane lets you configure SSL versions and encryption algorithms for clients and servers. It also lets you apply previously configured trustpoints to specific interfaces and configure a fallback trustpoint for interfaces that do not have an associated trustpoint.

Note For Release 9.3(2), SSLv3 has been deprecated. The default is now **tlsv1** instead of **any**. The **any** keyword has been deprecated. If you choose **any**, **sslv3**, or **sslv3-only**, the settings are accepted with a warning. Click **OK** to continue. In the next major ASA release, these keywords will be removed from the ASA.

For Version 9.4(1), all SSLv3 keywords have been removed from the ASA configuration, and SSLv3 support has been removed from the ASA. If you have SSLv3 enabled, a boot-time error will appear from the command with the SSLv3 option. The ASA will then revert to the default use of TLSv1.

The Citrix mobile receiver may not support TLS 1.1/1.2 protocols; see https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf for compatibility

Fields

- **Server SSL Version**—Specify the minimum SSL/TLS protocol version that the ASA uses when acting as a server from the drop-down list.

Any	Accepts SSLv2 client hellos and negotiates the highest common version.
SSL V3	Accepts SSLv2 client hellos and negotiates SSLv3 (or greater).

TLS V1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
TLSV1.3	Accepts SSLv2 client hellos and negotiates TLSv1.3 (or greater).
DTLSv1	Accepts DTLSv1 client hellos and negotiates DTLSv1 (or greater)
DTLS1.2	Accepts DTLSv1.2 client hellos and negotiates DTLSv1.2 (or greater)



Note The configuration and use of DTLS applies to the AnyConnect VPN Client connections only.

Ensure the TLS session is as secure, or more secure than the DTLS session by using an equal or higher version of TLS than DTLS. DTLSV1.2 supports TLSV1.2 and TLSV1.3. Any TLS version can be used with DTLS1 since they are all equal to or greater than DTLS 1. However, if you configure the server-max-version with TLSV1.2 or lower, the ASDM connection terminates.

TLSV1.3 requires Cisco Secure Client, Version 5.0 and above.

- **Client SSL Version**—Specify the minimum SSL/TLS protocol version that the ASA uses when acting as a client from the drop-down list. (DTLS not available for SSL client role)

Any	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
SSL V3	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
TLS V1	Transmits TLSv1 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Transmits TLSv1.1 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Transmits TLSv1.2 client hellos and negotiates TLSv1.2 (or greater).
TLSV1.3	Transmits TLSv1.3 client hellos and negotiates TLSv1.3 (or greater).

- **Diffie-Hellmann group to be used with SSL**—Choose a group from the drop-down list. Available options are Group1 - 768-bit modulus, Group2 - 1024-bit modulus, Group5 - 1536-bit modulus, Group14 - 2048-bit modulus, 224-bit prime order, and Group24 - 2048-bit modulus, 256-bit prime order. The default is Group2.
- **ECDH group to be used with SSL**—Choose a group from the drop-down list. Available options are Group19 - 256-bit EC, Group20 - 384-bit EC, and Group21 - 521-bit EC. The default value is Group19.



Note ECDSA and DHE ciphers are the highest priority.

- **Encryption**—Specify the version, security level, and SSL encryption algorithms that you want to support. Click **Edit** to define or modify a table entry using the Configure Cipher Algorithms/Custom String dialog box. Choose the SSL cipher security level, then click **OK**.
  - **Cipher Version**—Lists the cipher version that the ASA supports and uses for SSL connections.
  - **Cipher Security Level**—Lists the cipher security levels that the ASA supports and uses for SSL connections. Choose one of the following options:

    All includes all ciphers, including NULL-SHA.

    Low includes all ciphers, except NULL-SHA.

    Medium includes all ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5 (this is the default), RC4-SHA, and DES-CBC3-SHA.

    High includes AES-256 with SHA-2 ciphers and applies only to TLS version 1.2 and the ciphers supported by TLS version 1.3.

    Custom includes one or more ciphers that you specify in the Cipher algorithms/custom string box. This option provides you with full control of the cipher suite using OpenSSL cipher definition strings.
  - **Cipher Algorithms/Custom String**—Lists the cipher algorithms that the ASA supports and uses for SSL connections. For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/manmaster/man1/ciphers.html.

    The ASA specifies the order of priority for supported ciphers as: Ciphers supported by TLSv1.3/TLSv1.2 only, then ciphers not supported by TLSv1.1, TLSv1.2, or TLSv1.2.

  The following ciphers are supported:

- **Server Name Indication (SNI)**—Specifies the domain name and to associate with that domain. Click **Add** or **Edit** to define or modify a domain and trustpoint for each interface using the Add/Edit Server Name Indication (SNI) dialog box.

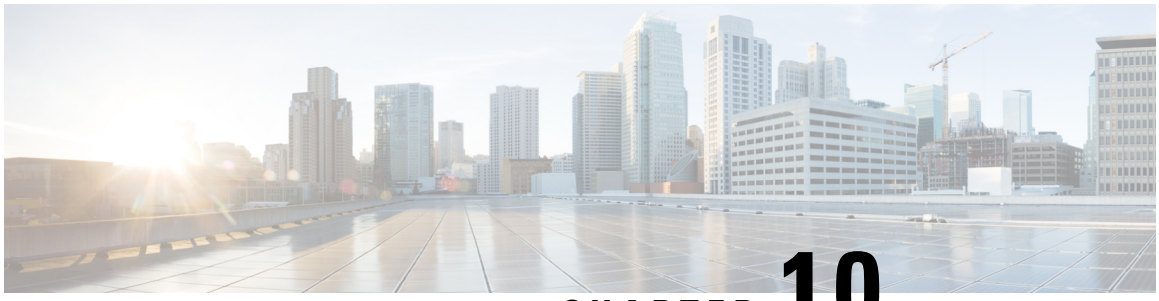
Cipher	TLSv1.1 / DTLS V1	TLSV1.2 / DTLSV 1.2
AES128-GCM-SHA256	no	yes
AES128-SHA	yes	yes
AES128-SHA256	no	yes
AES256-GCM-SHA384	no	yes
AES256-SHA	yes	yes
AES256-SHA256	no	yes
DERS-CBC-SHA	no	no
DES-CBC-SHA	yes	yes
DHE-RSA-AES128-GCM-SHA256	no	yes
DHE-RSA-AES128-SHA	yes	yes
DHE-RSA-AES128-SHA256	no	yes
DHE-RSA-AES256-GCM-SHA384	no	l

Cipher	TLSv1.1 / DTLS V1	TLSV1.2 / DTLSV 1.2
DHE-RSA-AES256-SHA	yes	yes
ECDHE-ECDSA-AES128-GCM-SHA256	no	yes
ECDHE-ECDSA-AES128-SHA256	no	yes
ECDHE-ECDSA-AES256-GCM-SHA384	no	yes
ECDHE-ECDSA-AES256-SHA384	no	yes
ECDHE-RSA-AES128-GCM-SHA256	yes	yes
ECDHE-RSA-AES128-SHA256	no	yes
ECDHE-RSA-AES256-GCM-SHA384	no	yes
ECDHE-RSA-AES256-SHA384	no	yes
NULL-SHA	no	no
RC4-MD5	no	no
RC4-SHA	no	no

Note DTLS1.2 tunnel works with TLSv1.3, however, DTLS1.2 does not support the TLSv1.3 ciphers. The highest priority supported cipher is chosen for the DTLS1.2 tunnel.

  - Specify domain—Enter the domain name.
  - Select trustpoint to associate with domain—Choose the trustpoint from the drop-down list.

- **Certificates—**Assign certificates to use for SSL authentication on each interface. Click **Edit** to define or modify the trustpoint for each interface using the Select SSL Certificate dialog box.
  - Primary Enrolled Certificate—Select the trustpoint to use for certificates on this interface.
  - Load Balancing Enrolled Certificate—Select a trustpoint to be used for certificates when VPN load balancing is configured.
- **Fallback Certificate**—Click to choose a certificate to use for interfaces that have no certificate associated with them. If you choose **None**, the ASA uses the default RSA key-pair and certificate.
- **Forced Certification Authentication Timeout**—Configure the number of minutes to wait before timing out certificate authentication.
- **Apply—**Click to save your changes.
- **Reset**—Click to remove changes you have made and reset SSL parameters to the previously defined values.



CHAPTER 10

Virtual Tunnel Interface

This chapter describes how to configure a VTI tunnel.

- About Virtual Tunnel Interfaces, on page 213
- Guidelines for Virtual Tunnel Interfaces, on page 213
- Create a VTI Tunnel, on page 215
- Feature History for Virtual Tunnel Interface, on page 220

About Virtual Tunnel Interfaces

ASA supports a logical interface called the Virtual Tunnel Interface (VTI). As an alternative to policy-based VPN, you can create a VPN tunnel between peers using VTIs. VTIs support route-based VPN with IPsec profiles attached to the end of each tunnel. You can use dynamic or static routes. Egressing traffic from the VTI is encrypted and sent to the peer, and the associated SA decrypts the ingress traffic to the VTI.

Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. You no longer have to track all remote subnets and include them in the crypto map access list. Deployments become easier, and having static VTI which supports route-based VPN with dynamic routing protocol also satisfies many requirements of a virtual private cloud.

Static VTI

You can use static VTI configurations for site-to-site connectivity in which a tunnel is always-on between two sites. For a static VTI interface, you must define a physical interface as a tunnel source. You can associate a maximum of 1024 VTIs per device. To create a static VTI interface, see Add a VTI Interface, on page 218.

Guidelines for Virtual Tunnel Interfaces

Context Mode and Clustering

- Supported in single mode only.
- No support for clustering.

Firewall Mode

Supported in routed mode only.

IPv6 Support

- IPv6 addressed VTIs can be configured.
- Both the tunnel source and the tunnel destination of a VTI can have IPv6 addresses.
- Following combinations of VTI IP (or internal networks IP version) over public IP versions are supported:
  - IPv6 over IPv6
  - IPv4 over IPv6
  - IPv4 over IPv4
  - IPv6 over IPv4
- Only static IPv6 address is supported as the tunnel source and destination.
- IPv6 BGP is not supported over VTI.
- The tunnel source interface can have IPv6 addresses and you can specify which address to be used as the tunnel endpoint. If you do not specify, by default, the first IPv6 global address in the list is used as the tunnel endpoint.
- You can specify the tunnel mode as IPv6. When specified, the IPv6 traffic can be tunneled through the VTI. However, the tunnel mode can either be IPv4 or IPv6 for a single VTI.

Bidirectional Forwarding Detection (BFD) for IPsec tunnel interface Guidelines

- For a Static VTI interface with a BFD template, configure only one IP address type, either IPv4 or IPv6. If the BFD neighbor does not come up due to dual IP address types, remove and re-add the tunnel interface with a single IP address type.
- Enable BFD only on the tunnel interface for Static VTI interface and on the tunnel group for Dynamic VTI interface. You must not configure BFD neighbor under router BGP for the same overlay neighbor IP address.
- For BFD-enabled tunnels, set the Dead Peer Detection (DPD) interval to 60 seconds or more, depending on the total number of BFD tunnels on the device.

General Configuration Guidelines

- VTIs are only configurable in IPsec mode. To terminate GRE tunnels on an ASA is unsupported.
- You can use BGP or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface. However, if you change the physical interface MTU after the VTI is enabled, you must disable and reenable the VTI to use the new MTU setting.
- For static VTIs, you can configure a maximum of 1024 VTIs on a device. While calculating the VTI count, consider the following:
  - Include nameif subinterfaces to derive the total number of VTIs that can be configured on the device.

  - You cannot configure nameif on member interfaces of a portchannel. Therefore, the tunnel count is reduced by the count of actual main portchannel interfaces alone and not any of its member interfaces.
  - Even if a platform supports more than 1024 interfaces, the VTI count is limited to the number of VLANs configurable on that platform. For example, if a model supports 500 VLANs, then the tunnel count would be 500 minus the number of physical interfaces configured.

- VTI supports IKE versions v1, v2, and uses IPsec for sending and receiving data between the tunnel's source and destination.
- If NAT has to be applied, the IKE and ESP packets are encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- The tunnel group name must match what the peer sends as its IKEv1 or IKEv2 identity.
- For IKEv1 in site-to-site tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- Access rules can be applied on a VTI interface to control traffic through VTI.
- ICMP ping is supported between VTI interfaces.
- If the peer device for an IKEv2 site-to-site VPN tunnel sends IKEv2 configuration request payloads, the ASA cannot establish an IKEv2 tunnel with the device. You must disable the config-exchange request on the peer device for the ASA to establish a VPN tunnel with the peer device.

Default Settings

- By default, all traffic through VTI is encrypted.
- By default, the security level for VTI interfaces is 0. You cannot configure the security level.

Limitations for VTI

ASA drops Security Group Tag (SGT) frames and packets after VTI decryption.

Create a VTI Tunnel

To configure a VTI tunnel, create an IPsec proposal (transform set). You will need to create an IPsec profile that references the IPsec proposal, followed by a VTI interface with the IPsec profile. Configure the remote peer with identical IPsec proposal and IPsec profile parameters. SA negotiation will start when all tunnel parameters are configured.

Note For the ASA which is a part of both the VPN VTI domains, and has BGP adjacency on the physical interface:

When a state change is triggered due to the interface health check, the routes in the physical interface will be deleted until BGP adjacency is re-established with the new active peer. This behavior does not apply to logical VTI interfaces.

Access control lists can be applied on a VTI interface to control traffic through VTI. To permit any packets that come from an IPsec tunnel without checking ACLs for the source and destination interfaces, enter the sysopt connection permit-vpn command in global configuration mode.

You can use the following command to enable IPsec traffic through the ASA without checking ACLs:

hostname(config)# sysopt connection permit-vpn

When an outside interface and VTI interface have the security level of 0, if you have ACL applied on VTI interface, it will not be hit if you do not have same-security-traffic configured.

To configure this feature, use the **same-security-traffic** command in global configuration mode with its **intra-interface** argument.

Procedure

Step 1 Add an IPsec Proposal (Transform Sets).

Step 2 Add an IPsec Profile.

Step 3 Add a VTI Tunnel.

Add an IPsec Proposal (Transform Sets)

A transform set is required to secure traffic in a VTI tunnel. Used as a part of the IPsec profile, it is a set of security protocols and algorithms that protects the traffic in the VPN.

Before you begin

- You can use either pre-shared key or certificates for authenticating the IKE session associated with a VTI. IKEv2 allows asymmetric authentication methods and keys. For both IKEv1 and IKEv2, you must configure the pre-shared key under the tunnel group used for the VTI.
- For certificate based authentication using IKEv1, you must specify the trustpoint to be used at the initiator. For the responder, you must configure the trustpoint in the tunnel-group command. For IKEv2, you must configure the trustpoint to be used for authentication under the tunnel group command for both initiator and responder.

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)**.

Step 2 Configure IKEv1 or IKEv2 to establish the security association.

- Configure IKEv1.

a) In the IKEv1 IPsec Proposals (Transform Sets) panel, click **Add**.
b) Enter the **Set Name**.
c) Retain the default selection of the **Tunnel** check box.
d) Select **ESP Encryption** and **ESP Authentication**.
e) Click **OK**.

- Configure IKEv2.

a) In the IKEv2 IPsec Proposals panel, click **Add**.
b) Enter the **Name**, and **Encryption**.
c) Choose the **Integrity Hash**.
d) Click **OK**.

Add an IPsec Profile

An IPsec profile contains the required security protocols and algorithms in the IPsec proposal or transform set that it references. This ensures a secure, logical communication path between two site-to-site VTI VPN peers.

Procedure

Step 1 Choose **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)**.

Step 2 In the **IPsec Profile** panel, click **Add**.

Step 3 Enter the IPsec profile **Name**.

Step 4 Enter the **IKE v1 IPsec Proposal** or the **IKE v2 IPsec Proposal** created for the IPsec profile. You can choose either an IKEv1 transform set or an IKEv2 IPsec proposal.

Step 5 If you need an end of the VTI tunnel to act only as a responder, check the **Responder only** check box.

- You can configure one end of the VTI tunnel to perform only as a responder. The responder-only end will not initiate the tunnel or rekeying.
- If you are using IKEv2, set the duration of the security association lifetime greater than the lifetime value in the IPsec profile in the initiator end. This is to facilitate successful rekeying by the initiator end and ensure that the tunnels remain up.
- If the rekey configuration in the initiator end is unknown, remove the responder-only mode to make the SA establishment bi-directional, or configure an infinite IPsec lifetime value in the responder-only end to prevent expiry.

Step 6 (Optional) Check the **Enable security association lifetime** check box, and enter the security association duration values in **kilobytes** and **seconds**.

Step 7 (Optional) Check the **PFS Settings** check box to enable PFS, and select the required Diffie-Hellman Group.

Perfect Forward Secrecy (PFS) generates a unique session key for each encrypted exchange. This unique session key protects the exchange from subsequent decryption. To configure PFS, you have to select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key. The key derivation algorithms generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus provides higher security, but requires more processing time. You must have matching Diffie-Hellman groups on both peers.

This establishes the strength of the of the encryption-key-determination algorithm. The ASA uses this algorithm to derive the encryption and hash keys.

Step 8 (Optional) Check the **Enable sending certificate** check box, and select a **Trustpoint** that defines the certificate to be used while initiating a VTI tunnel connection. Check the **Chain** check box, if required.

Step 9 Click **OK**.

Step 10 In the **IPsec Proposals (Transform Sets)** main panel, click **Apply**.

Step 11 In the **Preview CLI Commands** dialog box, click **Send**.

Add a VTI Interface

To create a new VTI interface and establish a VTI tunnel, perform the following steps:



Note Implement IP SLA to ensure that the tunnel remains up when a router in the active tunnel is unavailable. See Configure Static Route Tracking in the ASA General Operations Configuration Guide in http://www.cisco.com/go/asa-config.

Procedure

Step 1 Choose **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Step 2 Choose **Add** > **VTI Interface**. The **Add VTI Interface** window appears.

Step 3 In the **General** tab:

a) Enter the **VTI ID**. The range is from 0 to 10413. Up to 10413 VTI interfaces are supported.

b) Enter the **Interface Name**.

c) Ensure that the **Enable Interface** check box is checked.

d) Choose **IPv4** or **IPv6** from the **Path Monitoring** drop-down list and enter the IP address of the peer.

e) Enter the **Cost**. The range is from 1 to 65535.

The cost determines the priority to load balance the traffic across multiple VTIs. The lowest number has the highest priority.

f) For configuring the IP address:

Click the **Address** radio button to configure an IP address and the subnet mask.

Or

Click the **Unnumbered** radio button to choose an interface from the **IP Unnumbered** drop-down list to borrow its IP address. You can choose a loopback interface or a physical interface from the list.

Step 4 In the **Advanced** tab.

a) Enter the **Destination IP**.

b) Choose the tunnel source interface from the **Source Interface** drop-down list.

You can select a loopback interface or a physical interface.

c) Select the IPsec policy in the **Tunnel Protection with IPsec Policy** field.

d) Select the IPsec profile in the **Tunnel Protection with IPsec Profile** field.

e) Check the **Ensure the Enable Tunnel Mode IPv4 IPsec** check box.

Step 5 Click **OK**.

Step 6 In the **Interfaces** panel, click **Apply**.

Step 7 In the **Preview CLI Commands** dialog box, click **Send**.

After the updated configuration is loaded, the new VTI appears in the list of interfaces. This new VTI can be used to create an IPsec site-to-site VPN.

Example

Example configuration of a VTI tunnel (with IKEv2) between ASA and an IOS device:

```
ASA:

crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 group 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]
```

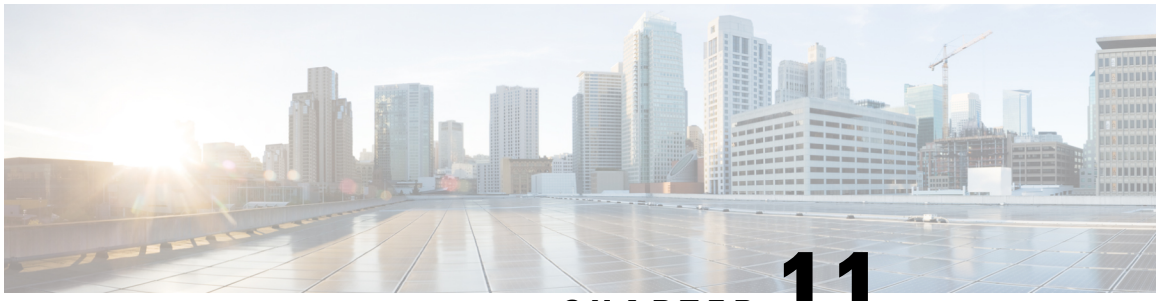
```
IOS:

!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 group 21
!
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
 ip address 10.10.10.0 255.255.255.254
 tunnel mode ipsec ipv4
 tunnel source [router-interface]
 tunnel destination [asa-ip-address]
 tunnel protection ipsec profile asa-vti
!
```

Feature History for Virtual Tunnel Interface

Feature Name	Releases	Feature Information
Local tunnel ID support	9.17(1)	ASA supports unique local tunnel ID that allows ASA to have multiple IPsec tunnel behind a NAT to connect to Cisco Umbrella Secure Internet Gateway (SIG). The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels.
Support for IPv6 on Static VTI	9.16(1)	ASA supports IPv6 addresses in Virtual Tunnel Interfaces (VTI) configurations. A VTI tunnel source interface can have an IPv6 address, which you can configure to use as the tunnel endpoint. If the tunnel source interface has multiple IPv6 addresses, you can specify which address to be used, else the first IPv6 global address in the list is used by default. The tunnel mode can be either IPv4 or IPv6, but it must be the same as IP address type configured on VTI for the tunnel to be active. An IPv6 address can be assigned to the tunnel source or the tunnel destination interface in a VTI.

Feature Name	Releases	Feature Information
Support for 1024 VTI interfaces per device	9.16(1)	The number of maximum VTIs to be configured on a device has been increased from 100 to 1024. Even if a platform supports more than 1024 interfaces, the VTI count is limited to the number of VLANs configurable on that platform. For example, ASA 5510 supports 100 VLANs, the tunnel count would be 100 minus the number of physical interfaces configured. New/Modified screens: None
DHCP Relay Server Support on VTI	9.14(1)	ASA allows VTI interfaces to be configured as DHCP relay server connecting interfaces. We modified the following screen to specify a VTI interface for DHCP relay: **Configuration** > **Device Management** > **DHCP** > **DHCP Relay** > **DHCP Relay Interface Servers**
Support for IKEv2, certificate based authentication, and ACL in VTI	9.8.(1)	Virtual Tunnel Interface (VTI) now supports BGP (static VTI). You can now use IKEv2 in standalone and high availability modes. You can use certificate based authentication by setting up a trustpoint in the IPsec profile. You can also apply access lists on VTI using access-group commands to filter ingress traffic. We introduced options to select the trustpoint for certificate based authentication in the following screen: **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** > **Add**
Virtual Tunnel Interface (VTI) support	9.7.(1)	The ASA is enhanced with a new logical interface called Virtual Tunnel Interface (VTI), used to represent a VPN tunnel to a peer. This supports route based VPN with IPsec profiles attached to each end of the tunnel. Using VTI does away with the need to configure static crypto map access lists and map them to interfaces. We introduced the following screens: **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** > **Add** > **Add IPsec Profile** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** > **General** **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VTI Interface** > **Advanced**



CHAPTER 11

Configure an External AAA Server for VPN

- About External AAA Servers, on page 223
- Guidelines For Using External AAA Servers, on page 224
- Configure Multiple Certificate Authentication, on page 224
- Active Directory/LDAP VPN Remote Access Authorization Examples, on page 225

About External AAA Servers

This ASA can be configured to use an external LDAP, RADIUS, or TACACS+ server to support Authentication, Authorization, and Accounting (AAA) for the ASA. The external AAA server enforces configured permissions and attributes. Before you configure the ASA to use an external server, you must configure the external AAA server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.

Understanding Policy Enforcement of Authorization Attributes

The ASA supports several methods of applying user authorization attributes (also called user entitlements or permissions) to VPN connections. You can configure the ASA to obtain user attributes from any combination of:

- a Dynamic Access Policy (DAP) on the ASA
- an external RADIUS or LDAP authentication and/or authorization server
- a group policy on the ASA

If the ASA receives attributes from all sources, the attributes are evaluated, merged, and applied to the user policy. If there are conflicts between attributes, the DAP attributes take precedence.

The ASA applies attributes in the following order:

1. DAP attributes on the ASA—Introduced in Version 8.0(2), these attributes take precedence over all others. If you set a bookmark or URL list in DAP, it overrides a bookmark or URL list set in the group policy.
2. User attributes on the AAA server—The server returns these attributes after successful user authentication and/or authorization. Do not confuse these with attributes that are set for individual users in the local AAA database on the ASA (User Accounts in ASDM).

3. Group policy configured on the ASA—If a RADIUS server returns the value of the RADIUS CLASS attribute IETF-Class-25 (OU=*group-policy*) for the user, the ASA places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

   For LDAP servers, any attribute name can be used to set the group policy for the session. The LDAP attribute map that you configure on the ASA maps the LDAP attribute to the Cisco attribute IETF-Radius-Class.

4. Group policy assigned by the Connection Profile (called tunnel-group in the CLI)—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication. All users connecting to the ASA initially belong to this group, which provides any attributes that are missing from the DAP, user attributes returned by the server, or the group policy assigned to the user.

5. Default group policy assigned by the ASA (DfltGrpPolicy)—System default attributes provide any values that are missing from the DAP, user attributes, group policy, or connection profile.

Guidelines For Using External AAA Servers

The ASA enforces the LDAP attributes based on attribute name, not numeric ID. RADIUS attributes, are enforced by numeric ID, not by name.

For ASDM Version 7.0, LDAP attributes include the cVPN3000 prefix. For ASDM Versions 7.1 and later, this prefix was removed.

LDAP attributes are a subset of the Radius attributes, which are listed in the Radius chapter.

Configure Multiple Certificate Authentication

You can now validate multiple certificates per session with the AnyConnect Client SSL and IKEv2 client protocols. For example, you can make sure that the issuer name of the machine certificate matches a particular CA and therefore that the device is a corporate-issued device.

The multiple certificates option allows certificate authentication of both the machine and user via certificates. Without this option, you could only do certificate authentication of one or the other, but not both.



Note Because multiple certificate authentication requires a machine certificate and a user certificate (or two user certificates), you cannot use AnyConnect Client start before logon (SBL) with this feature.

The pre-fill username field allows a field from the second (user) certificate to be parsed and used for subsequent AAA authentication in a AAA and certificate authenticated connection. The username for both primary and secondary prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to specify which certificate the primary and secondary username should come from when configuring multiple certificate authentication and using the pre-fill username option for Authentication or Authorization. For information, see AnyConnect Client Connection Profile, Authentication Attributes, on page 99

With multiple certificate authentication, two certificates are authenticated: the second (user) certificate received from the client is the one that the pre-fill and username-from-certificate primary and secondary usernames are parsed from.

You can also configure multiple certificate authentication with SAML.

With multiple-certificate authentication, you can make policy decisions based on the fields of a certificate used to authenticate that connection attempt. The user and machine certificate received from the client during multiple-certificate authentication is loaded into DAP to allow policies to be configured based on the field of the certificate. To add multiple certificate authentication using Dynamic Access Policies (DAP) so that you can set up rules to allow or disallow connection attempts, refer to *Add Multiple Certificate Authentication to DAP* in the appropriate release of the ASA VPN ASDM Configuration Guide.

Active Directory/LDAP VPN Remote Access Authorization Examples

This section presents example procedures for configuring authentication and authorization on the ASA using the Microsoft Active Directory server. It includes the following topics:

- Policy Enforcement of User-Based Attributes, on page 225
- Enforce Static IP Address Assignment for AnyConnect Client Tunnels, on page 227
- Enforce Dial-in Allow or Deny Access, on page 228
- Enforce Logon Hours and Time-of-Day Rules, on page 231

Other configuration examples available on Cisco.com include the following TechNotes.

- ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example
- PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login

Policy Enforcement of User-Based Attributes

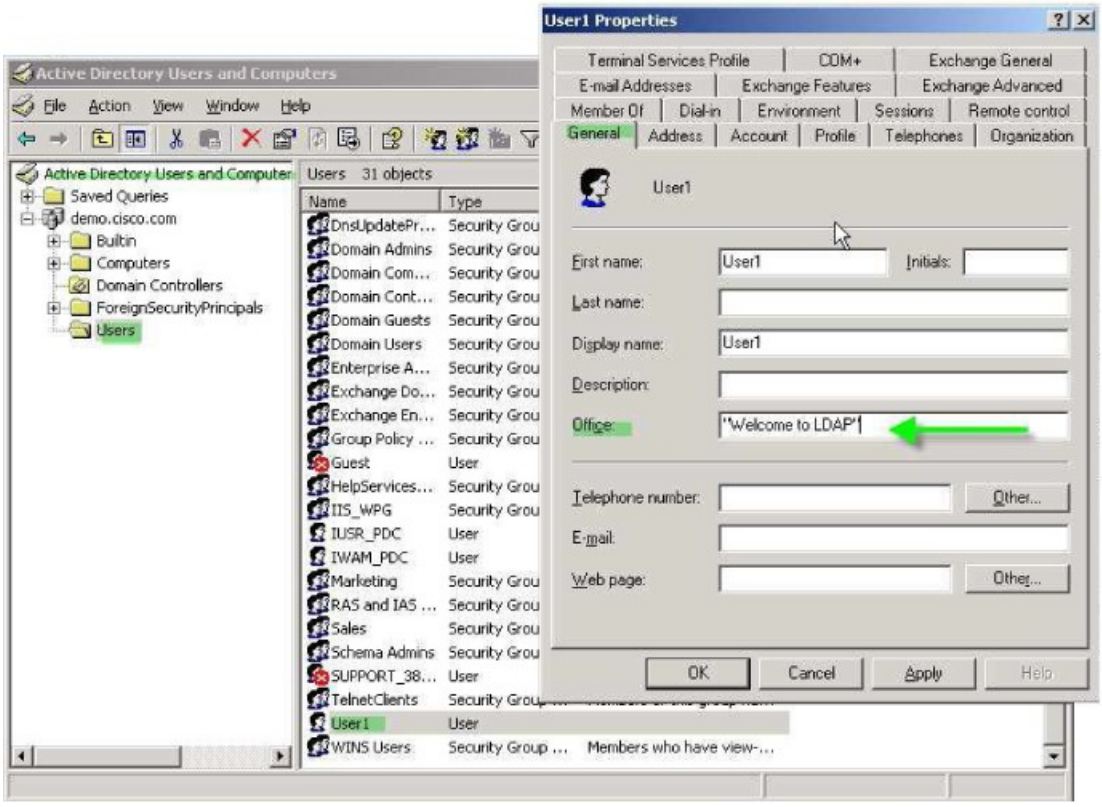
This example displays a simple banner to the user, showing how you can map any standard LDAP attribute to a well-known Vendor-Specific Attribute (VSA), and you can map one or more LDAP attribute(s) to one or more Cisco LDAP attributes. It applies to any connection type, including the IPsec VPN client and AnyConnect Client.

To enforce a simple banner for a user who is configured on an AD LDAP server use the Office field in the General tab to enter the banner text. This field uses the attribute named physicalDeliveryOfficeName. On the ASA, create an attribute map that maps physicalDeliveryOfficeName to the Cisco attribute Banner1.

During authentication, the ASA retrieves the value of physicalDeliveryOfficeName from the server, maps the value to the Cisco attribute Banner1, and displays the banner to the user.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **General** tab and enter banner text in the Office field, which uses the AD/LDAP attribute physicalDeliveryOfficeName.



Step 2 Create an LDAP attribute map on the ASA.

Create the map Banner and map the AD/LDAP attribute physicalDeliveryOfficeName to the Cisco attribute Banner1:

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associate the attribute map Banner that you previously created:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

Step 4 Test the banner enforcement.

Enforce Static IP Address Assignment for AnyConnect Client Tunnels

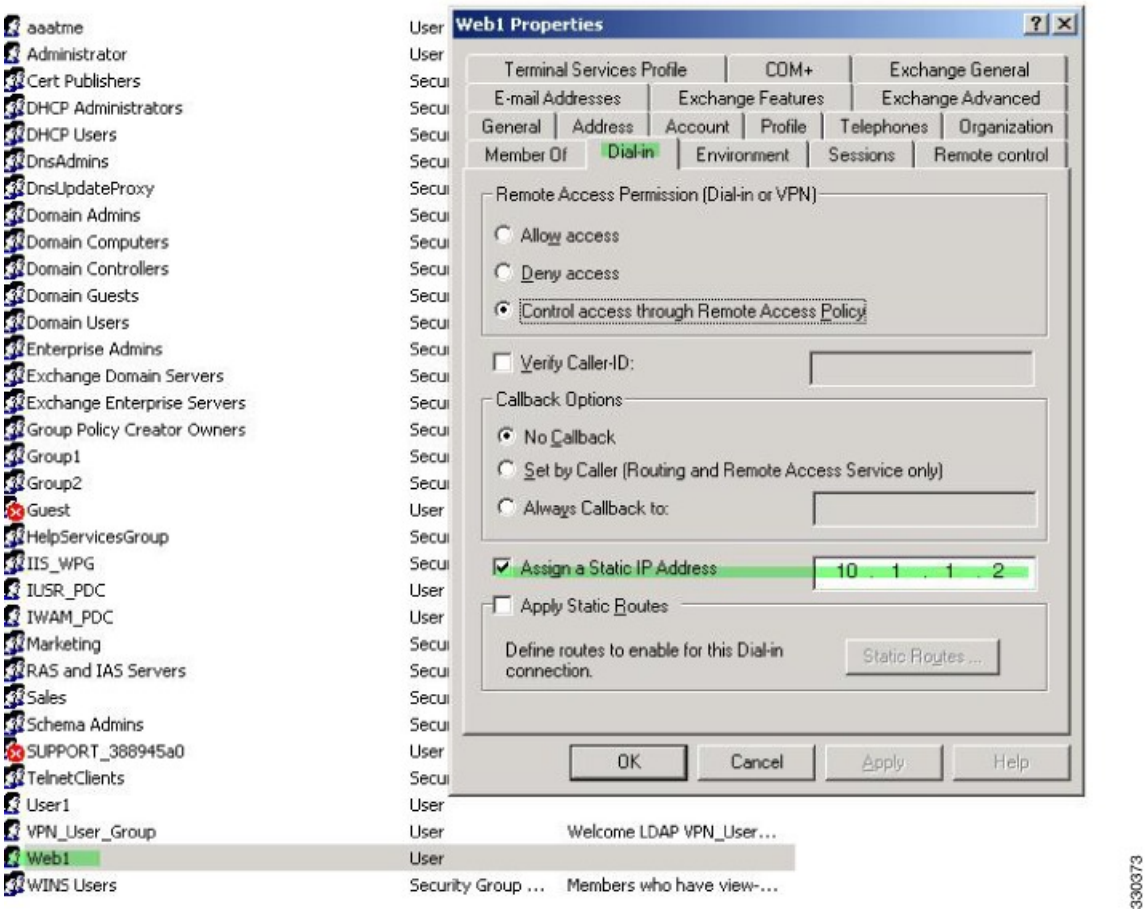
This example applies to full-tunnel clients, such as the IPsec client and the SSL VPN clients.

To enforce static AnyConnect Client static IP assignments configure the AnyConnect Client user Web1 to receive a static IP address, enter the address in the Assign Static IP Address field of the Dialin tab on the AD LDAP server (this field uses the msRADIUSFramedIPAddress attribute), and create an attribute map that maps this attribute to the Cisco attribute IETF-Radius-Framed-IP-Address.

During authentication, the ASA retrieves the value of msRADIUSFramedIPAddress from the server, maps the value to the Cisco attribute IETF-Radius-Framed-IP-Address, and provides the static address to User1.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, check the **Assign Static IP Address** check box, and enter an IP address of 10.1.1.2.



Step 2 Create an attribute map for the LDAP configuration shown.

Map the AD attribute msRADIUSFramedIPAddress used by the Static Address field to the Cisco attribute IETF-Radius-Framed-IP-Address:

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associates the attribute map static_address that you previously created in:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

Step 4 Verify that the **vpn-address-assignment** command is configured to specify AAA by viewing this part of the configuration:

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

Step 5 Establish a connection to the ASA with the AnyConnect Client. Observe that the user receives the IP address configured on the server and mapped to the ASA.

Step 6 Use the **show vpn-sessiondb svc** command to view the session details and verify the address assigned:

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Enforce Dial-in Allow or Deny Access

This example creates an LDAP attribute map that specifies the tunneling protocols allowed by the user. You map the allow access and deny access settings on the Dialin tab to the Cisco attribute Tunneling-Protocol, which supports the following bitmap values:

Value	Tunneling Protocol
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	Clientless SSL
32	SSL client—AnyConnect Client or SSL VPN client
64	IPsec (IKEv2)

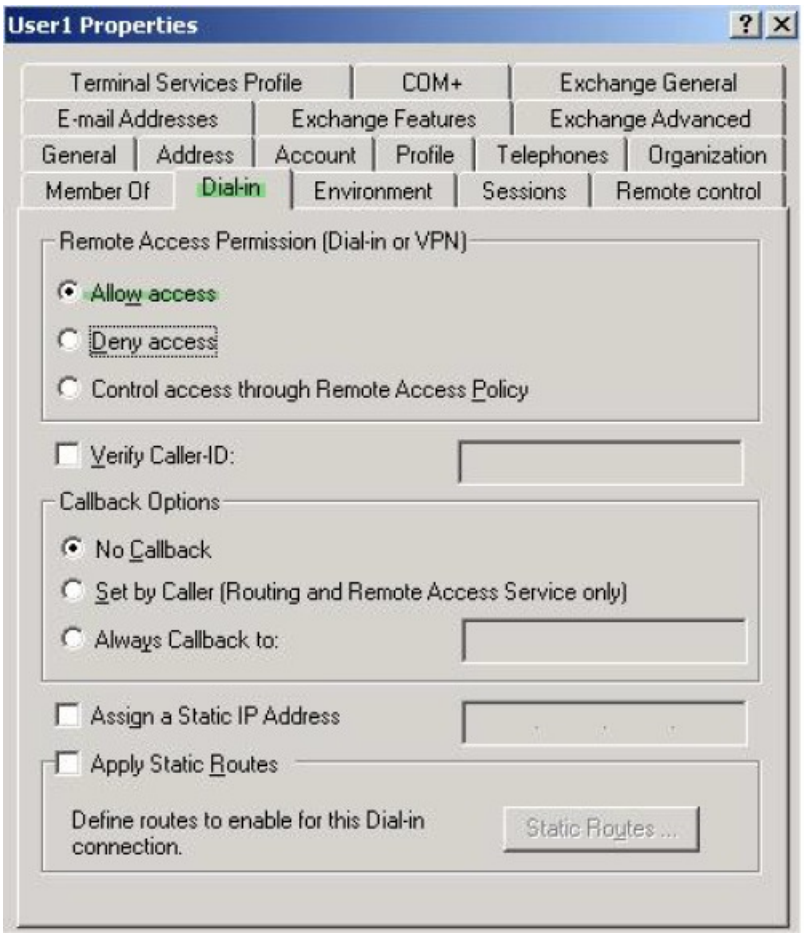
[1] (1) IPsec and L2TP over IPsec are not supported simultaneously. Therefore, the values 4 and 8 are mutually exclusive.
[2] (2) See note 1.

Use this attribute to create an Allow Access (TRUE) or a Deny Access (FALSE) condition for the protocols, and enforce the method for which the user is allowed access.

See Tech Note ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example for another example of enforcing dial-in allow access or deny access.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, and click the Allow Access radio button.



Note
If you choose the Control access through the Remote Access Policy option, then a value is not returned from the server, and the permissions that are enforced are based on the internal group policy settings of the ASA.

Step 2 Create an attribute map to allow both an IPsec and AnyConnect Client connection, but deny a clientless SSL connection.

a) Create the map tunneling_protocols:

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Map the AD attribute msNPAllowDialin used by the Allow Access setting to the Cisco attribute Tunneling-Protocols:

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Add map values:

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

Step 3 Associate the LDAP attribute map to the AAA server.

a) Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associates the attribute map tunneling_protocols that you created:

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

Step 4 Verify that the attribute map works as configured.

Try connections using clientless SSL, the user should be informed that an unauthorized connection mechanism was the reason for the failed connection. The IPsec client should connect because IPsec is an allowed tunneling protocol according to the attribute map.

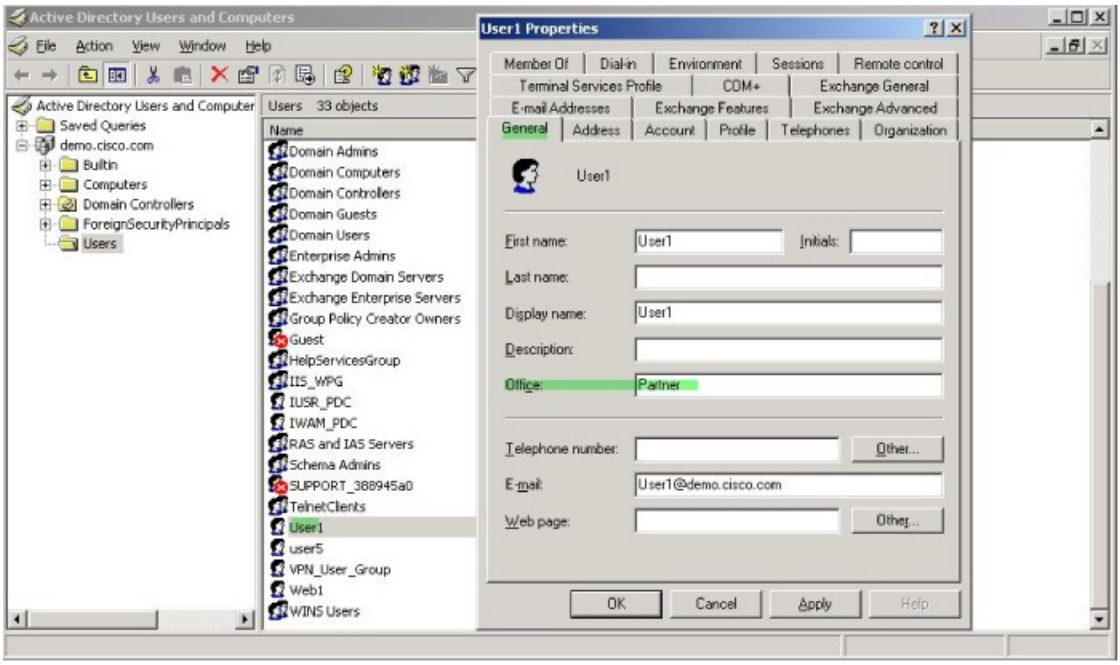
Enforce Logon Hours and Time-of-Day Rules

The following example shows how to configure and enforce the hours that a clientless SSL user (such as a business partner) is allowed to access the network.

On the AD server, use the Office field to enter the name of the partner, which uses the physicalDeliveryOfficeName attribute. Then we create an attribute map on the ASA to map that attribute to the Cisco attribute Access-Hours. During authentication, the ASA retrieves the value of physicalDeliveryOfficeName and maps it to Access-Hours.

Procedure

Step 1 Select the user, right-click **Properties**, and open the **General** tab:



Step 2 Create an attribute map.

Create the attribute map access_hours and map the AD attribute physicalDeliveryOfficeName used by the Office field to the Cisco attribute Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for host 10.1.1.2 in the AAA server group MS_LDAP and associate the attribute map access_hours that you created.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

Step 4 Configure time ranges for each value allowed on the server.

Configure Partner access hours from 9am to 5pm Monday through Friday:

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```