



Cisco ASDM User Guide

Version 6.1

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

Text Part Number: OL-16647-01

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

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

Cisco ASDM User Guide

© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xxxix

Related Documentation xxxix

Document Conventions xxxix

Obtaining Documentation and Submitting a Service Request xl

PART 1

Getting Started

CHAPTER 1

Welcome to ASDM 1-1

Multiple ASDM Session Support 1-1

Caveats 1-1

Unsupported Commands 1-2

Ignored and View-Only Commands 1-2

Effects of Unsupported Commands 1-3

About the ASDM Interface 1-3

Menus 1-4

File Menu 1-4

View Menu 1-5

Tools Menu 1-6

Wizards Menu 1-6

Window Menu 1-7

Help Menu 1-7

Toolbar 1-7

ASDM Assistant 1-8

Status Bar 1-9

Connection to Device 1-9

Device List 1-9

Common Buttons 1-10

Keyboard Shortcuts 1-11

Enabling Extended Screen Reader Support 1-12

Organizational Folder 1-13

About the Help Window 1-13

Header Buttons 1-13

Browser Window 1-13

Home Pane 1-14

Device Dashboard Tab	1-15
Firewall Dashboard Tab	1-17
Content Security Tab	1-18
Intrusion Prevention Tab	1-20
Connecting to IPS	1-20
System Home Pane	1-21

CHAPTER 2

Introduction to the Security Appliance 2-1

New Features by Platform Release	2-1
New Features in Version 8.1(1)	2-2
New Features in Version 8.0(4)	2-2
New Features in Version 8.0(3)	2-5
New Features in Version 8.0(2)	2-6
Firewall Functional Overview	2-12
Security Policy Overview	2-12
Permitting or Denying Traffic with Access Lists	2-13
Applying NAT	2-13
Protecting from IP Fragments	2-13
Using AAA for Through Traffic	2-13
Applying HTTP, HTTPS, or FTP Filtering	2-13
Applying Application Inspection	2-13
Sending Traffic to the Advanced Inspection and Prevention Security Services Module	2-14
Sending Traffic to the Content Security and Control Security Services Module	2-14
Applying QoS Policies	2-14
Applying Connection Limits and TCP Normalization	2-14
Enabling Threat Detection	2-14
Firewall Mode Overview	2-15
Stateful Inspection Overview	2-15
VPN Functional Overview	2-16
Security Context Overview	2-16

CHAPTER 3

Defining Preferences and Using Configuration, Diagnostic, and File Management Tools 3-1

Preferences	3-1
Configuration Tools	3-3
Reset Device to the Factory Default Configuration	3-3
Save Running Configuration to TFTP Server	3-4
Save Internal Log Buffer to Flash	3-5
Command Line Interface	3-5
Command Errors	3-6

Interactive Commands	3-6
Avoiding Conflicts with Other Administrators	3-6
Show Commands Ignored by ASDM on Device	3-6
Diagnostic Tools	3-7
Packet Tracer	3-7
Ping	3-8
Using the Ping Tool	3-9
Troubleshooting the Ping Tool	3-10
Traceroute	3-11
Administrator's Alert to Clientless SSL VPN Users	3-12
ASDM Java Console	3-12
Packet Capture Wizard	3-13
Field Information for the Packet Capture Wizard	3-14
File Management Tools	3-18
File Management	3-18
Manage Mount Points	3-19
Add/Edit a CIFS/FTP Mount Point	3-19
Upgrade Software from Local Computer	3-20
File Transfer	3-21
Upgrade Software from Cisco.com Wizard	3-23
ASDM Assistant	3-24
System Reload	3-25
Backup and Restore	3-26
Backing Up Configurations	3-26
Restoring Configurations	3-27

CHAPTER 4

Before You Start 4-1

Factory Default Configurations	4-1
Restoring the Factory Default Configuration	4-1
ASA 5505 Default Configuration	4-2
ASA 5510 and Higher Version Default Configuration	4-3
PIX 515/515E Default Configuration	4-4
Configuring the Security Appliance for ASDM Access	4-4
Setting Transparent or Routed Firewall Mode at the CLI	4-4
Starting ASDM	4-6
Downloading the ASDM Launcher	4-6
Starting ASDM from the ASDM Launcher	4-6
Using ASDM in Demo Mode	4-7
Starting ASDM from a Web Browser	4-8

Configuration Overview 4-9

PART 2

Device Setup and Management

CHAPTER 5

Using the Startup Wizard 5-1

Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances 5-2

Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance 5-2

Step 1 - Starting Point or Welcome 5-3

Step 2 - Basic Configuration 5-4

Step 3 - Auto Update Server 5-5

Step 4 - Management IP Address Configuration 5-6

Step 5 - Interface Selection 5-6

Step 6 - Switch Port Allocation 5-7

Step 7 - Interface IP Address Configuration 5-8

Step 8 - Internet Interface Configuration - PPPoE 5-9

Step 9 - Business Interface Configuration - PPPoE 5-10

Step 10 - Home Interface Configuration - PPPoE 5-11

Step 11 - General Interface Configuration 5-12

Step 12 - Static Routes 5-13

Add/Edit Static Routes 5-13

Step 13 - DHCP Server 5-13

Step 14 - Address Translation (NAT/PAT) 5-14

Step 15 - Administrative Access 5-15

Add/Edit Administrative Access Entry 5-16

Step 16 - Easy VPN Remote Configuration 5-17

Step 17 - Startup Wizard Summary 5-19

Other Interfaces Configuration 5-19

Edit Interface 5-20

Interface Configuration 5-20

Outside Interface Configuration - PPPoE 5-21

Outside Interface Configuration 5-22

CHAPTER 6

Configuring Basic Device Settings 6-1

Management IP Address 6-1

System Time 6-2

Clock 6-2

NTP 6-3

Add/Edit NTP Server Configuration 6-4

Configuring Advanced Device Management Features 6-4

Configuring HTTP Redirect	6-4
Edit HTTP/HTTPS Settings	6-5
Configuring Maximum SSL VPN Sessions	6-5
History Metrics	6-6
System Image/Configuration	6-6
Activation Key	6-6
Auto Update	6-7
Set Polling Schedule	6-9
Add/Edit Auto Update Server	6-9
Advanced Auto Update Settings	6-10
Boot Image/Configuration	6-10
Add Boot Image	6-11
Device Name/Password	6-12
System Software	6-13
Add/Edit Client Update	6-14

CHAPTER 7
Configuring Interfaces in Single Mode 7-1

Interface Overview	7-1
Physical Interface Overview	7-1
Default Physical Interface Settings	7-2
Connector Types	7-2
Auto-MDI/MDIX Feature	7-2
Redundant Interface Overview	7-2
Redundant Interfaces and Failover Guidelines	7-2
Redundant Interface MAC Address	7-3
Physical Interface Guidelines for Use in a Redundant Interface	7-3
VLAN Subinterface and 802.1Q Trunking Overview	7-3
Maximum Subinterfaces	7-4
Preventing Untagged Packets on the Physical Interface	7-4
Default State of Interfaces	7-4
Default Security Level	7-4
Configuring an Interface (Single Mode)	7-5
Enabling Same Security Level Communication (Single Mode)	7-8
PPPoE IP Address and Route Settings	7-9

CHAPTER 8
Configuring Interfaces in Multiple Mode 8-1

Configuring Interfaces in the System Configuration (Multiple Mode)	8-1
Configuring Physical Interfaces in the System Configuration (Multiple Mode)	8-2
Physical Interface Overview	8-2

Configuring and Enabling Physical Interfaces in the System Configuration (Multiple Mode)	8-3
Configuring Redundant Interfaces in the System Configuration (Multiple Mode)	8-3
Redundant Interface Overview	8-4
Adding a Redundant Interface in the System Configuration (Multiple Mode)	8-5
Configuring VLAN Subinterfaces and 802.1Q Trunking in the System Configuration (Multiple Mode)	8-5
Subinterface Overview	8-5
Adding a Subinterface in the System Configuration (Multiple Mode)	8-6
Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration (Multiple Mode)	8-7
Allocating Interfaces to Contexts	8-7
Configuring Interface Parameters within each Context (Multiple Mode)	8-7
Interface Parameters Overview	8-7
Default State of Interfaces	8-8
Default Security Level	8-8
Configuring Interface Parameters in each Context (Multiple Mode)	8-9
Enabling Same Security Level Communication (Multiple Mode)	8-10

CHAPTER 9

Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance 9-1

Interface Overview	9-1
Understanding ASA 5505 Ports and Interfaces	9-2
Maximum Active VLAN Interfaces for Your License	9-2
Default Interface Configuration	9-4
VLAN MAC Addresses	9-4
Power Over Ethernet	9-4
Monitoring Traffic Using SPAN	9-4
Security Level Overview	9-5
Configuring VLAN Interfaces	9-5
Interfaces > Interfaces	9-6
Add/Edit Interface > General	9-8
Add/Edit Interface > Advanced	9-10
Configuring Switch Ports	9-11
Interfaces > Switch Ports	9-11
Edit Switch Port	9-12

CHAPTER 10

Configuring Security Contexts 10-1

Security Context Overview	10-1
Common Uses for Security Contexts	10-2
Unsupported Features	10-2

Context Configuration Files	10-2
How the Security Appliance Classifies Packets	10-2
Valid Classifier Criteria	10-3
Invalid Classifier Criteria	10-4
Classification Examples	10-4
Cascading Security Contexts	10-7
Management Access to Security Contexts	10-8
System Administrator Access	10-8
Context Administrator Access	10-9
Enabling or Disabling Multiple Context Mode	10-9
Backing Up the Single Mode Configuration	10-9
Enabling Multiple Context Mode	10-9
Restoring Single Context Mode	10-10
Configuring Resource Classes	10-10
Classes and Class Members Overview	10-11
Resource Limits	10-11
Default Class	10-12
Class Members	10-13
Adding a Resource Class	10-13
Monitoring Context Resource Usage	10-15
Configuring Security Contexts	10-16
Adding a Security Context	10-16
Automatically Assigning MAC Addresses	10-17
MAC Address Overview	10-18
Enabling Automatic MAC Address Assignment	10-18

CHAPTER 11

Configuring Dynamic And Static Routing 11-1

Dynamic Routing	11-1
OSPF	11-1
Setup	11-2
Filtering	11-8
Interface	11-10
Redistribution	11-14
Static Neighbor	11-17
Summary Address	11-18
Virtual Link	11-19
RIP	11-22
Setup	11-23
Interface	11-24

Filter Rules	11-25
Redistribution	11-27
EIGRP	11-28
Configuring EIGRP	11-29
Field Information for the EIGRP Panes	11-30
Static Routes	11-40
Static Route Tracking	11-41
Configuring Static Route Tracking	11-42
Field Information for Static Routes	11-42
Static Routes	11-42
Add/Edit Static Route	11-43
Route Monitoring Options	11-44
ASR Group	11-45
Proxy ARPs	11-46

CHAPTER 12

Configuring Multicast Routing 12-1

Multicast	12-1
IGMP	12-2
Access Group	12-2
Add/Edit Access Group	12-3
Join Group	12-3
Add/Edit IGMP Join Group	12-4
Protocol	12-5
Configure IGMP Parameters	12-5
Static Group	12-6
Add/Edit IGMP Static Group	12-7
Multicast Route	12-7
Add/Edit Multicast Route	12-8
MBoundary	12-9
Edit Boundary Filter	12-9
Add/Edit/Insert Neighbor Filter Entry	12-10
MForwarding	12-11
PIM	12-11
Protocol	12-12
Edit PIM Protocol	12-12
Neighbor Filter	12-13
Add/Edit/Insert Neighbor Filter Entry	12-14
Bidirectional Neighbor Filter	12-14
Add/Edit/Insert Bidirectional Neighbor Filter Entry	12-15

Rendezvous Points	12-16
Add/Edit Rendezvous Point	12-16
Request Filter	12-18
Request Filter Entry	12-19
Route Tree	12-20

CHAPTER 13

DHCP, DNS and WCCP Services 13-1

DHCP Relay	13-1
Edit DHCP Relay Agent Settings	13-3
Add/Edit Global DHCP Relay Server	13-3
DHCP Server	13-4
Edit DHCP Server	13-6
Advanced DHCP Options	13-7
DNS Client	13-9
Add/Edit DNS Server Group	13-9
Dynamic DNS	13-10
Add/Edit Dynamic DNS Update Methods	13-12
Add/Edit Dynamic DNS Interface Settings	13-12
WCCP	13-13
WCCP Service Groups	13-13
Add or Edit WCCP Service Group	13-14
Redirection	13-14
Add or Edit WCCP Redirection	13-15

CHAPTER 14

Configuring AAA Servers and the Local Database 14-1

AAA Overview	14-1
About Authentication	14-2
About Authorization	14-2
About Accounting	14-2
AAA Server and Local Database Support	14-3
Summary of Support	14-3
RADIUS Server Support	14-4
Authentication Methods	14-4
Attribute Support	14-4
RADIUS Authorization Functions	14-4
TACACS+ Server Support	14-4
SDI Server Support	14-5
SDI Version Support	14-5
Two-step Authentication Process	14-5

SDI Primary and Replica Servers	14-5
NT Server Support	14-5
Kerberos Server Support	14-5
LDAP Server Support	14-6
Authentication with LDAP	14-6
Securing LDAP Authentication with SASL	14-6
LDAP Server Types	14-7
Authorization with LDAP for VPN	14-7
SSO Support for WebVPN with HTTP Forms	14-7
Local Database Support	14-8
User Profiles	14-8
Fallback Support	14-8
Configuring AAA Server Groups	14-9
Adding a Server Group	14-9
Adding a Server to a Group	14-10
AAA Server Parameters	14-11
RADIUS Server Fields	14-11
TACACS+ Server Fields	14-13
SDI Server Fields	14-13
Windows NT Domain Server Fields	14-13
Kerberos Server Fields	14-14
LDAP Server Fields	14-14
HTTP Form Server Fields	14-16
Testing Server Authentication and Authorization	14-16
Adding a User Account	14-17
Configuring VPN Policy Attributes for a User	14-19
Configuring LDAP Attribute Maps	14-21
Adding an Authentication Prompt	14-22

CHAPTER 15

High Availability 15-1

Understanding Failover	15-1
Active/Standby Failover	15-2
Active/Active Failover	15-2
Stateless (Regular) Failover	15-3
Stateful Failover	15-3
Configuring Failover with the High Availability and Scalability Wizard	15-4
Accessing and Using the High Availability and Scalability Wizard	15-4
Configuring Active/Active Failover with the High Availability and Scalability Wizard	15-4
Configuring Active/Standby Failover with the High Availability and Scalability Wizard	15-5

Configuring VPN Load Balancing with the High Availability and Scalability Wizard	15-6
Field Information for the High Availability and Scalability Wizard	15-7
Choose the Type of Failover Configuration	15-7
Check Failover Peer Connectivity and Compatibility	15-8
Change Device to Multiple Mode	15-8
Select Failover Communication Media	15-9
Security Context Configuration	15-9
Failover Link Configuration	15-10
State Link Configuration	15-11
Standby Address Configuration	15-11
VPN Cluster Load Balancing Configuration	15-12
Summary	15-14
Field Information for the Failover Panes	15-14
Failover - Single Mode	15-15
Failover: Setup	15-15
Failover: Interfaces (Routed Firewall Mode)	15-17
Failover: Interfaces (Transparent Firewall Mode)	15-19
Failover: Criteria	15-20
Failover: MAC Addresses	15-21
Add/Edit Interface MAC Address	15-22
Failover-Multiple Mode, Security Context	15-23
Failover - Routed	15-23
Failover - Transparent	15-24
Failover-Multiple Mode, System	15-26
Failover > Setup Tab	15-26
Failover > Criteria Tab	15-28
Failover > Active/Active Tab	15-29
Failover > MAC Addresses Tab	15-32

CHAPTER 16

Configuring Management Access 16-1

Configuring Device Access	16-1
Configuring CLI Parameters	16-2
Adding a Banner	16-2
Customizing a CLI Prompt	16-3
Changing the Console Timeout Period	16-4
Configuring File Access	16-4
Configuring the FTP Client Mode	16-4
Configuring the Security Appliance as a Secure Copy Server	16-5
Configuring the Security Appliance as a TFTP Client	16-5

Adding Mount Points	16-6
Adding a CIFS Mount Point	16-6
Adding an FTP Mount Point	16-6
Configuring ICMP Access	16-7
Configuring a Management Interface	16-9
Configuring SNMP	16-9
Information About SNMP	16-9
Information About SNMP Terminology	16-10
Information About the Management Information Base and Traps	16-10
Configuring an SNMP Agent and Management Station	16-17
Configuring the SNMP Agent	16-18
Adding an SNMP Management Station	16-18
Configuring SNMP Traps	16-19
Configuring Management Access Rules	16-19
Configuring AAA for System Administrators	16-20
Configuring Authentication for CLI, ASDM, and enable command Access	16-20
Limiting User CLI and ASDM Access with Management Authorization	16-22
Configuring Command Authorization	16-23
Command Authorization Overview	16-23
About Preserving User Credentials	16-23
Configuring Local Command Authorization	16-25
Configuring TACACS+ Command Authorization	16-27
Configuring Management Access Accounting	16-31
Recovering from a Lockout	16-32

CHAPTER 17

Configuring Logging 17-1

About Logging	17-1
Security Contexts in Logging	17-1
Using Logging	17-2
Logging Setup	17-2
Configure FTP Settings	17-3
Configure Logging Flash Usage	17-4
Syslog Setup	17-4
Edit Syslog ID Settings	17-5
Advanced Syslog Configuration	17-6
E-Mail Setup	17-7
Add/Edit E-Mail Recipients	17-7
Event Lists	17-8

Add/Edit Event List	17-10
Add/Edit Syslog Message ID Filter	17-10
Logging Filters	17-10
Edit Logging Filters	17-11
Add/Edit Class and Severity Filter	17-12
Add/Edit Syslog Message ID Filter	17-13
Rate Limit	17-14
Edit Rate Limit for Syslog Logging Level	17-15
Add/Edit Rate Limit for Syslog Message	17-15
Syslog Servers	17-16
Add/Edit Syslog Server	17-17
SMTP	17-17
Using NetFlow	17-18

PART 3

Configuring the Firewall

CHAPTER 18

Firewall Mode Overview	18-1
Routed Mode Overview	18-1
IP Routing Support	18-1
Transparent Mode Overview	18-1
Transparent Firewall Network	18-2
Allowing Layer 3 Traffic	18-2
Allowed MAC Addresses	18-2
Passing Traffic Not Allowed in Routed Mode	18-2
MAC Address vs. Route Lookups	18-3
Using the Transparent Firewall in Your Network	18-4
Transparent Firewall Guidelines	18-4
Unsupported Features in Transparent Mode	18-5

CHAPTER 19

Adding Global Objects	19-1
Using Network Objects and Groups	19-1
Network Object Overview	19-2
Configuring a Network Object	19-2
Configuring a Network Object Group	19-3
Using Network Objects and Groups in a Rule	19-4
Viewing the Usage of a Network Object or Group	19-4
Configuring Service Groups	19-5
Service Groups	19-5

Add/Edit Service Group	19-6
Browse Service Groups	19-7
Configuring Class Maps	19-8
Configuring Inspect Maps	19-8
Configuring Regular Expressions	19-8
Regular Expressions	19-8
Add/Edit Regular Expression	19-9
Build Regular Expression	19-11
Test Regular Expression	19-13
Add/Edit Regular Expression Class Map	19-14
Configuring TCP Maps	19-14
Configuring Global Pools	19-14
Configuring Time Ranges	19-15
Add/Edit Time Range	19-15
Add/Edit Recurring Time Range	19-16
Encrypted Traffic Inspection	19-17
TLS Proxy	19-17
Configure TLS Proxy Pane	19-19
Adding a TLS Proxy Instance	19-20
Add TLS Proxy Instance Wizard – Server Configuration	19-20
Add TLS Proxy Instance Wizard – Client Configuration	19-22
Add TLS Proxy Instance Wizard – Other Steps	19-23
Phone Proxy	19-24
Configuring the Phone Proxy	19-24
Creating a Phone Proxy Instance	19-24
Add/Edit TFTP Server	19-26
CTL File	19-27
Creating a CTL File	19-28
Add/Edit Record Entry	19-28
CTL Provider	19-29
Add/Edit CTL Provider	19-30
CHAPTER 20	
Configuring Access Rules and EtherType Rules	20-1
Information About Access Rules and EtherType Rules	20-1
Information About Both Access Rules and EtherType Rules	20-2
Using Access Rules and EtherType Rules on the Same Interface	20-2
Rule Order	20-2
Implicit Deny	20-2

Inbound and Outbound Rules	20-2
Information About Access Rules	20-3
IP Addresses Used for Access Rules When You Use NAT	20-4
Access Rules for Returning Traffic	20-6
Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules	20-6
Information About EtherType Rules	20-6
Supported EtherTypes	20-6
Implicit Permit of IP and ARPs Only	20-7
IPv6 Unsupported	20-7
Allowing MPLS	20-7
Configuring Access Rules	20-7
Rule Queries	20-10
New/Edit Rule Query	20-10
Add/Edit Access Rule	20-11
Manage Service Groups	20-12
Add/Edit Service Group	20-13
Advanced Access Rule Configuration	20-13
Log Options	20-14
Configuring EtherType Rules (Transparent Mode Only)	20-15
Add/Edit EtherType Rule	20-16

CHAPTER 21

Configuring NAT	21-1
NAT Overview	21-1
Introduction to NAT	21-1
NAT in Routed Mode	21-2
NAT in Transparent Mode	21-3
NAT Control	21-4
NAT Types	21-6
Dynamic NAT	21-6
PAT	21-8
Static NAT	21-8
Static PAT	21-9
Bypassing NAT When NAT Control is Enabled	21-10
Policy NAT	21-10
NAT and Same Security Level Interfaces	21-12
Order of NAT Rules Used to Match Real Addresses	21-13
Mapped Address Guidelines	21-13
DNS and NAT	21-13

Configuring NAT Control	21-15
Using Dynamic NAT	21-16
Dynamic NAT Implementation	21-16
Real Addresses and Global Pools Paired Using a Pool ID	21-17
NAT Rules on Different Interfaces with the Same Global Pools	21-17
Global Pools on Different Interfaces with the Same Pool ID	21-18
Multiple NAT Rules with Different Global Pools on the Same Interface	21-18
Multiple Addresses in the Same Global Pool	21-19
Outside NAT	21-20
Real Addresses in a NAT Rule Must be Translated on All Lower or Same Security Interfaces	21-21
Managing Global Pools	21-21
Configuring Dynamic NAT, PAT, or Identity NAT	21-22
Configuring Dynamic Policy NAT or PAT	21-24
Using Static NAT	21-25
Configuring Static NAT, PAT, or Identity NAT	21-26
Configuring Static Policy NAT, PAT, or Identity NAT	21-28
Using NAT Exemption	21-30

CHAPTER 22

Configuring Service Policy Rules 22-1

Service Policy Overview	22-1
Supported Features	22-1
Service Policy Elements	22-2
Default Global Policy	22-2
Feature Directionality	22-3
Feature Matching Guidelines	22-3
Order in Which Multiple Feature Actions within a Rule are Applied	22-4
Incompatibility of Certain Feature Actions	22-5
Feature Matching Guidelines for Multiple Service Policies	22-5
Adding a Service Policy Rule for Through Traffic	22-6
Adding a Service Policy Rule for Management Traffic	22-10
RADIUS Accounting Inspection Overview	22-10
Configuring a Service Policy Rule for Management Traffic	22-10
Managing the Order of Service Policy Rules	22-13
RADIUS Accounting Field Descriptions	22-14
Select RADIUS Accounting Map	22-14
Add RADIUS Accounting Policy Map	22-15
RADIUS Inspect Map	22-16
RADIUS Inspect Map Host	22-16

RADIUS Inspect Map Other 22-17

CHAPTER 23

Applying AAA for Network Access 23-1

AAA Performance 23-1

Configuring Authentication for Network Access 23-1

Information About Authentication 23-2

One-Time Authentication 23-2

Applications Required to Receive an Authentication Challenge 23-2

Security Appliance Authentication Prompts 23-2

Static PAT and HTTP 23-3

Configuring Network Access Authentication 23-4

Enabling the Redirection Method of Authentication for HTTP and HTTPS 23-5

Enabling Secure Authentication of Web Clients 23-5

Authenticating Directly with the Security Appliance 23-6

Authenticating Telnet Connections with a Virtual Server 23-7

Authenticating HTTP(S) Connections with a Virtual Server 23-7

Configuring the Authentication Proxy Limit 23-9

Configuring Authorization for Network Access 23-9

Configuring TACACS+ Authorization 23-9

Configuring RADIUS Authorization 23-10

Configuring a RADIUS Server to Send Downloadable Access Control Lists 23-11

Configuring a RADIUS Server to Download Per-User Access Control List Names 23-15

Configuring Accounting for Network Access 23-15

Using MAC Addresses to Exempt Traffic from Authentication and Authorization 23-16

CHAPTER 24

Configuring Application Layer Protocol Inspection 24-1

Inspection Engine Overview 24-2

When to Use Application Protocol Inspection 24-2

Inspection Limitations 24-3

Default Inspection Policy 24-3

Configuring Application Inspection 24-4

CTIQBE Inspection 24-5

CTIQBE Inspection Overview 24-5

Limitations and Restrictions 24-5

DCERPC Inspection 24-6

DNS Inspection 24-6

How DNS Application Inspection Works 24-6

How DNS Rewrite Works 24-7

ESMTP Inspection	24-8
FTP Inspection	24-8
FTP Inspection Overview	24-8
Using Strict FTP	24-9
Verifying and Monitoring FTP Inspection	24-10
GTP Inspection	24-10
H.323 Inspection	24-11
H.323 Inspection Overview	24-12
How H.323 Works	24-12
Limitations and Restrictions	24-13
HTTP Inspection	24-13
Instant Messaging Inspection	24-14
ICMP Inspection	24-14
ICMP Error Inspection	24-14
ILS Inspection	24-14
MGCP Inspection	24-15
MMP Inspection	24-17
Configuring MMP Inspection for a TLS Proxy	24-18
NetBIOS Inspection	24-18
PPTP Inspection	24-19
RADIUS Accounting Inspection	24-19
RSH Inspection	24-19
RTSP Inspection	24-19
RTSP Inspection Overview	24-20
Using RealPlayer	24-20
Restrictions and Limitations	24-20
SIP Inspection	24-21
SIP Inspection Overview	24-21
SIP Instant Messaging	24-21
Skinny (SCCP) Inspection	24-22
SCCP Inspection Overview	24-23
Supporting Cisco IP Phones	24-23
Restrictions and Limitations	24-24
SMTP and Extended SMTP Inspection	24-24
SNMP Inspection	24-25
SQL *Net Inspection	24-25
Sun RPC Inspection	24-26

Sun RPC Inspection Overview	24-26
SUNRPC Server	24-26
Add/Edit SUNRPC Service	24-27
TFTP Inspection	24-28
XDMCP Inspection	24-28
Service Policy Field Descriptions	24-28
Rule Actions > Protocol Inspection Tab	24-29
Select DCERPC Map	24-31
Select DNS Map	24-31
Select ESMTP Map	24-32
Select FTP Map	24-32
Select GTP Map	24-33
Select H.323 Map	24-33
Select HTTP Map	24-34
Select IM Map	24-34
Select IPSec-Pass-Thru Map	24-35
Select MGCP Map	24-35
Select NETBIOS Map	24-36
Select RTSP Map	24-36
Select SCCP (Skinny) Map	24-37
Select SIP Map	24-37
Select SNMP Map	24-38
Class Map Field Descriptions	24-39
DNS Class Map	24-39
Add/Edit DNS Traffic Class Map	24-40
Add/Edit DNS Match Criterion	24-40
Manage Regular Expressions	24-42
Manage Regular Expression Class Maps	24-42
FTP Class Map	24-43
Add/Edit FTP Traffic Class Map	24-44
Add/Edit FTP Match Criterion	24-44
H.323 Class Map	24-46
Add/Edit H.323 Traffic Class Map	24-46
Add/Edit H.323 Match Criterion	24-47
HTTP Class Map	24-48
Add/Edit HTTP Traffic Class Map	24-49
Add/Edit HTTP Match Criterion	24-49
IM Class Map	24-53
Add/Edit IM Traffic Class Map	24-54

Add/Edit IM Match Criterion	24-54
SIP Class Map	24-56
Add/Edit SIP Traffic Class Map	24-57
Add/Edit SIP Match Criterion	24-57
Inspect Map Field Descriptions	24-59
DCERPC Inspect Map	24-62
Add/Edit DCERPC Policy Map	24-63
DNS Inspect Map	24-64
Add/Edit DNS Policy Map (Security Level)	24-66
Add/Edit DNS Policy Map (Details)	24-67
Add/Edit DNS Inspect	24-69
Manage Class Maps	24-70
ESMTP Inspect Map	24-71
MIME File Type Filtering	24-72
Add/Edit ESMTP Policy Map (Security Level)	24-73
Add/Edit ESMTP Policy Map (Details)	24-74
Add/Edit ESMTP Inspect	24-75
FTP Inspect Map	24-79
File Type Filtering	24-80
Add/Edit FTP Policy Map (Security Level)	24-80
Add/Edit FTP Policy Map (Details)	24-81
Add/Edit FTP Map	24-82
GTP Inspect Map	24-84
IMSI Prefix Filtering	24-84
Add/Edit GTP Policy Map (Security Level)	24-85
Add/Edit GTP Policy Map (Details)	24-86
Add/Edit GTP Map	24-88
H.323 Inspect Map	24-89
Phone Number Filtering	24-90
Add/Edit H.323 Policy Map (Security Level)	24-91
Add/Edit H.323 Policy Map (Details)	24-92
Add/Edit HSI Group	24-93
Add/Edit H.323 Map	24-94
HTTP Inspect Map	24-95
URI Filtering	24-96
Add/Edit HTTP Policy Map (Security Level)	24-97
Add/Edit HTTP Policy Map (Details)	24-98
Add/Edit HTTP Map	24-99
Instant Messaging (IM) Inspect Map	24-103
Add/Edit Instant Messaging (IM) Policy Map	24-104

Add/Edit IM Map	24-104
IPSec Pass Through Inspect Map	24-106
Add/Edit IPSec Pass Thru Policy Map (Security Level)	24-107
Add/Edit IPSec Pass Thru Policy Map (Details)	24-108
MGCP Inspect Map	24-109
Gateways and Call Agents	24-109
Add/Edit MGCP Policy Map	24-110
Add/Edit MGCP Group	24-111
NetBIOS Inspect Map	24-112
Add/Edit NetBIOS Policy Map	24-112
RTSP Inspect Map	24-113
Add/Edit RTSP Policy Map	24-113
Add/Edit RTSP Inspect	24-114
SCCP (Skinny) Inspect Map	24-115
Message ID Filtering	24-116
Add/Edit SCCP (Skinny) Policy Map (Security Level)	24-117
Add/Edit SCCP (Skinny) Policy Map (Details)	24-118
Add/Edit Message ID Filter	24-119
SIP Inspect Map	24-120
Add/Edit SIP Policy Map (Security Level)	24-121
Add/Edit SIP Policy Map (Details)	24-122
Add/Edit SIP Inspect	24-124
SNMP Inspect Map	24-126
Add/Edit SNMP Map	24-127

CHAPTER 25

Configuring QoS 25-1

QoS Overview	25-1
Supported QoS Features	25-2
What is a Token Bucket?	25-2
Policing Overview	25-3
Priority Queueing Overview	25-3
Traffic Shaping Overview	25-4
How QoS Features Interact	25-4
DSCP and DiffServ Preservation	25-5
Creating the Standard Priority Queue for an Interface	25-5
Creating a Policy for Standard Priority Queueing and/or Policing	25-6
Creating a Policy for Traffic Shaping and Hierarchical Priority Queueing	25-7

CHAPTER 26**Configuring Filter Rules 26-1**

URL Filtering 26-1

Configuring URL Filtering 26-2

URL Filtering Servers 26-2

Add/Edit Parameters for Websense URL Filtering 26-3

Add/Edit Parameters for Secure Computing SmartFilter URL Filtering 26-4

Advanced URL Filtering 26-4

Filter Rules 26-5

Add/Edit Filter Rule 26-7

Filtering the Rule Table 26-9

Define Query 26-10

Browse Source/Destination/Service 26-11

CHAPTER 27**Configuring Advanced Firewall Protection 27-1**

Configuring Threat Detection 27-1

Configuring Basic Threat Detection 27-1

Basic Threat Detection Overview 27-2

Configuring Basic Threat Detection 27-2

Configuring Scanning Threat Detection 27-3

Configuring Threat Statistics 27-4

Threat Detection Field Descriptions 27-5

Configuring Connection Settings 27-6

Connection Limit Overview 27-6

TCP Intercept Overview 27-7

Disabling TCP Intercept for Management Packets for Clientless SSL VPN Compatibility 27-7

Dead Connection Detection Overview 27-7

TCP Sequence Randomization Overview 27-7

TCP Normalization Overview 27-8

Enabling Connection Limits and TCP Normalization 27-8

Configuring IP Audit 27-11

IP Audit Policy 27-11

Add/Edit IP Audit Policy Configuration 27-12

IP Audit Signatures 27-12

IP Audit Signature List 27-13

Configuring the Fragment Size 27-17

Show Fragment 27-18

Edit Fragment 27-19

Configuring Anti-Spoofing 27-20

Configuring TCP Options	27-20
TCP Reset Settings	27-22
Configuring Global Timeouts	27-23

CHAPTER 28

Configuring IPS 28-1

AIP SSM Overview	28-1
How the AIP SSM Works with the Adaptive Security Appliance	28-2
Operating Modes	28-2
Using Virtual Sensors	28-3
AIP SSM Procedure Overview	28-4
Accessing IDM from ASDM	28-5
Configuring the AIP SSM Security Policy in IDM	28-5
Assigning Virtual Sensors to Security Contexts	28-5
Diverting Traffic to the AIP SSM	28-6
Intrusion Prevention Tab Field Descriptions	28-7
Resetting the AIP SSM Password	28-8

CHAPTER 29

Configuring Trend Micro Content Security 29-1

Connecting to the CSC SSM	29-1
Managing the CSC SSM	29-2
About the CSC SSM	29-2
Getting Started with the CSC SSM	29-3
Determining What Traffic to Scan	29-5
Rule Actions for CSC Scanning	29-6
CSC SSM Setup	29-7
Activation/License	29-8
IP Configuration	29-9
Host/Notification Settings	29-9
Management Access Host/Networks	29-10
Password	29-11
Restoring the Default Password	29-12
Wizard Setup	29-13
CSC Setup Wizard Activation Codes Configuration	29-13
CSC Setup Wizard IP Configuration	29-14
CSC Setup Wizard Host Configuration	29-15
CSC Setup Wizard Management Access Configuration	29-15
CSC Setup Wizard Password Configuration	29-16
CSC Setup Wizard Traffic Selection for CSC Scan	29-16

CSC Setup Wizard Summary	29-18
Web	29-19
Mail	29-20
SMTP Tab	29-20
POP3 Tab	29-21
File Transfer	29-22
Updates	29-23

CHAPTER 30

Configuring ARP Inspection and Bridging Parameters 30-1

Configuring ARP Inspection	30-1
ARP Inspection	30-1
Edit ARP Inspection Entry	30-2
ARP Static Table	30-3
Add/Edit ARP Static Configuration	30-4
Customizing the MAC Address Table	30-4
MAC Address Table	30-4
Add/Edit MAC Address Entry	30-6
MAC Learning	30-6

PART 4

Configuring VPN

CHAPTER 31

SSL VPN Wizard 31-1

SSL VPN Feature	31-1
SSL VPN Interface	31-2
User Authentication	31-2
Group Policy	31-3
Bookmark List	31-3
IP Address Pools and Client Image	31-4
Summary	31-4

CHAPTER 32

VPN 32-1

VPN Wizard	32-1
VPN Tunnel Type	32-2
Remote Site Peer	32-3
IKE Policy	32-4
IPSec Encryption and Authentication	32-5
Hosts and Networks	32-6
Summary	32-7

Remote Access Client	32-7
VPN Client Authentication Method and Name	32-8
Client Authentication	32-9
New Authentication Server Group	32-10
User Accounts	32-11
Address Pool	32-11
Attributes Pushed to Client	32-12
Address Translation Exemption	32-12

CHAPTER 33

Configuring Certificates 33-1

CA Certificate Authentication	33-1
Add/Install a CA Certificate	33-2
Identity Certificates Authentication	33-6
Code-Signer Certificates	33-11
Local Certificate Authority	33-12
Manage User Certificates	33-18
Manage User Database	33-18

CHAPTER 34

IKE 34-1

IKE Parameters	34-1
IKE Policies	34-4
Add/Edit IKE Policy	34-5
Assignment Policy	34-6
Address Pools	34-7
Add/Edit IP Pool	34-8
IPsec	34-8
Crypto Maps	34-9
Create IPsec Rule/Tunnel Policy (Crypto Map) - Basic Tab	34-11
Create IPsec Rule/Tunnel Policy (Crypto Map) - Advanced Tab	34-12
Create IPsec Rule/Traffic Selection Tab	34-13
Pre-Fragmentation	34-16
Edit IPsec Pre-Fragmentation Policy	34-17
IPsec Transform Sets	34-17
Add/Edit Transform Set	34-18
Load Balancing	34-19
Setting Global NAC Parameters	34-22
Configuring Network Admission Control Policies	34-23
Add/Edit Posture Validation Exception	34-26

CHAPTER 35

General 35-1

Client Software	35-1
Edit Client Update Entry	35-3
Default Tunnel Gateway	35-4
Group Policies	35-4
Add/Edit External Group Policy	35-5
Add AAA Server Group	35-6
Adding or Editing a Remote Access Internal Group Policy, General Attributes	35-6
Configuring the Portal for a Group Policy	35-8
Configuring Customization for a Group Policy	35-10
Adding or Editing a Site-to-Site Internal Group Policy	35-11
Browse Time Range	35-11
Add/Edit Time Range	35-12
Add/Edit Recurring Time Range	35-13
ACL Manager	35-14
Standard ACL	35-14
Extended ACL	35-15
Add/Edit/Paste ACE	35-16
Browse Source/Destination Address	35-18
Browse Source/Destination Port	35-18
Add TCP Service Group	35-19
Browse ICMP	35-19
Add ICMP Group	35-20
Browse Other	35-21
Add Protocol Group	35-21
Add/Edit Internal Group Policy > Servers	35-22
Add/Edit Internal Group Policy > IPSec Client	35-22
Client Access Rules	35-23
Add/Edit Client Access Rule	35-23
Add/Edit Internal Group Policy > Client Configuration Tab	35-24
Add/Edit Internal Group Policy > Client Configuration Tab > General Client Parameters Tab	35-24
View/Config Banner	35-25
Add/Edit Internal Group Policy > Client Configuration Tab > Cisco Client Parameters Tab	35-26
Add or Edit Internal Group Policy > Advanced > IE Browser Proxy	35-27
Add/Edit Standard Access List Rule	35-28
Add/Edit Internal Group Policy > Client Firewall Tab	35-29
Add/Edit Internal Group Policy > Hardware Client Tab	35-31
Add/Edit Server and URL List	35-33

Add/Edit Server or URL	35-34
Configuring SSL VPN Connections	35-34
Setting the Basic Attributes for an SSL VPN Connection	35-35
Setting Advanced Attributes for an IPSec or SSL VPN Connection	35-36
Setting General Attributes for an IPSec or SSL VPN Connection	35-36
Configuring SSL VPN Client Connections	35-38
ACLs	35-41
Configuring Clientless SSL VPN Connections	35-42
Add or Edit Clientless SSL VPN Connections	35-43
Add or Edit Clientless SSL VPN Connections > Basic	35-43
Add or Edit Clientless SSL VPN Connections > Advanced	35-43
Add or Edit Clientless SSL VPN Connections > Advanced > General	35-44
Add or Edit Clientless SSL VPN Connection Profile or IPSec Connection Profiles > Advanced > Authentication	35-45
Assign Authentication Server Group to Interface	35-46
Add or Edit SSL VPN Connections > Advanced > Authorization	35-46
Assign Authorization Server Group to Interface	35-46
Add or Edit SSL VPN Connections > Advanced > SSL VPN	35-47
Add or Edit Clientless SSL VPN Connections > Advanced > SSL VPN	35-47
Add or Edit Clientless SSL VPN Connections > Advanced > Name Servers	35-48
Configure DNS Server Groups	35-48
Add or Edit Clientless SSL VPN Connections > Advanced > Clientless SSL VPN	35-49
IPSec Remote Access Connection Profiles	35-49
Add or Edit an IPSec Remote Access Connection Profile	35-50
Add or Edit IPSec Remote Access Connection Profile Basic	35-50
Mapping Certificates to IPSec or SSL VPN Connection Profiles	35-51
Configure Site-to-Site Tunnel Groups	35-54
Add/Edit Site-to-Site Connection	35-54
Adding or Editing a Site-to-Site Tunnel Group	35-55
Crypto Map Entry	35-56
Crypto Map Entry for Static Peer Address	35-57
Managing CA Certificates	35-58
Install Certificate	35-58
Configure Options for CA Certificate	35-59
Revocation Check Tab	35-59
Add/Edit Remote Access Connections > Advanced > General	35-59
Configuring Client Addressing	35-61
Add/Edit Tunnel Group > General Tab > Authentication	35-64
Add/Edit SSL VPN Connection > General > Authorization	35-65

Add/Edit SSL VPN Connections > Advanced > Accounting	35-66
Add/Edit Tunnel Group > General > Client Address Assignment	35-67
Add/Edit Tunnel Group > General > Advanced	35-67
Add/Edit Tunnel Group > IPsec for Remote Access > IPsec	35-68
Add/Edit Tunnel Group for Site-to-Site VPN	35-70
Add/Edit Tunnel Group > PPP	35-71
Add/Edit Tunnel Group > IPsec for LAN to LAN Access > General > Basic	35-71
Add/Edit Tunnel Group > IPsec for LAN to LAN Access > IPsec	35-73
Add/Edit Tunnel Group > Clientless SSL VPN Access > General > Basic	35-75
Add/Edit Tunnel Group > Clientless SSL VPN > Basic	35-76
Configuring Internal Group Policy IPsec Client Attributes	35-77
Configuring Client Addressing for SSL VPN Connections	35-78
Assign Address Pools to Interface	35-79
Select Address Pools	35-79
Add or Edit an IP Address Pool	35-79
Authenticating SSL VPN Connections	35-80
System Options	35-80
Configuring SSL VPN Connections, Advanced	35-81
Configuring Split Tunneling	35-81
Zone Labs Integrity Server	35-82
Easy VPN Remote	35-83
Advanced Easy VPN Properties	35-85

CHAPTER 36

Configuring Dynamic Access Policies 36-1

Understanding VPN Access Policies	36-1
DAP Support for Remote Access Connection Types	36-3
DAP and AAA	36-3
DAP and Endpoint Security	36-4
DAP Connection Sequence	36-6
Test Dynamic Access Policies	36-6
Add/Edit Dynamic Access Policies	36-7
Add/Edit AAA Attributes	36-12
Retrieve AD Groups from selected AD Server Group	36-14
Add/Edit Endpoint Attributes	36-14
Operator for Endpoint Category	36-21
DAP Examples	36-21
Using DAP to Define Network Resources	36-21
Using DAP to Apply a WebVPN ACL	36-22
Enforcing CSD Checks and Applying Policies via DAP	36-22

CHAPTER 37

Clientless SSL VPN End User Set-up	37-1
Requiring Usernames and Passwords	37-1
Communicating Security Tips	37-2
Configuring Remote Systems to Use Clientless SSL VPN Features	37-2
Capturing Clientless SSL VPN Data	37-7
Creating a Capture File	37-8
Using a Browser to Display Capture Data	37-8

CHAPTER 38

Clientless SSL VPN	38-1
Security Precautions	38-1
ACLs	38-2
Add ACL	38-3
Add/Edit ACE	38-3
Configuring the Setup for Cisco Secure Desktop	38-4
Configuring Application Helper	38-7
Auto Signon	38-9
Add/Edit Auto Signon Entry	38-10
Configuring Session Settings	38-11
Java Code Signer	38-12
Content Cache	38-12
Content Rewrite	38-13
Java Code Signer	38-14
Encoding	38-14
Configuring Web ACLs	38-17
Port Forwarding	38-18
Configuring the Use of External Proxy Servers	38-20
Configuring Proxy Bypass	38-22
DTLS Settings	38-23
SSL VPN Client Settings	38-24
Add/Replace SSL VPN Client Image	38-25
Upload Image	38-26
Add/Edit SSL VPN Client Profiles	38-26
Upload Package	38-27
Bypass Interface Access List	38-28
SSO Servers	38-28
Configuring SiteMinder and SAML Browser Post Profile	38-29
SAML POST SSO Server Configuration	38-29

Adding the Cisco Authentication Scheme to SiteMinder	38-30
Add/Edit SSO Servers	38-30
Clientless SSL VPN Access	38-31
Configuring Smart Tunnel Access	38-33
Configuring Customization Objects	38-39
Add Customization Object	38-40
Import/Export Customization Object	38-40
Creating XML-Based Portal Customization Objects and URL Lists	38-41
Understanding the XML Customization File Structure	38-41
Customization Example	38-45
Using the Customization Template	38-47
The Customization Template	38-48
Help Customization	38-60
Import/Export Application Help Content	38-63
Configuring Browser Access to Client-Server Plug-ins	38-64
Language Localization	38-72
AnyConnect Customization	38-75
Resources	38-75
Binary	38-76
Installs	38-76
Import/Export Language Localization	38-77
Configure GUI Customization Objects (Bookmark Lists)	38-78
Add/Edit Bookmark List	38-79
Add Bookmark Entry	38-80
Import/Export Bookmark List	38-81
Configure GUI Customization Objects (Web Contents)	38-81
Import/Export Web Content	38-82
Add/Edit Post Parameter	38-82
Clientless SSL VPN Macro Substitutions	38-83

CHAPTER 39

E-Mail Proxy 39-1

Configuring E-Mail Proxy	39-1
AAA	39-2
POP3S Tab	39-2
IMAP4S Tab	39-4
SMTPS Tab	39-5
Access	39-7
Edit E-Mail Proxy Access	39-7
Authentication	39-8

Default Servers 39-9

Delimiters 39-10

CHAPTER 40

Configuring SSL Settings 40-1

SSL 40-1

Edit SSL Certificate 40-2

SSL Certificates 40-3

PART 5

Monitoring the Security Appliance

CHAPTER 41

Monitoring Interfaces 41-1

ARP Table 41-1

DHCP 41-1

DHCP Server Table 41-2

DHCP Client Lease Information 41-2

DHCP Statistics 41-3

MAC Address Table 41-4

Dynamic ACLs 41-5

Interface Graphs 41-5

Graph/Table 41-8

PPPoE Client 41-8

interface connection 41-9

Track Status for 41-9

Monitoring Statistics for 41-9

CHAPTER 42

Monitoring VPN 42-1

VPN Connection Graphs 42-1

IPSec Tunnels 42-1

Sessions 42-2

VPN Statistics 42-3

Sessions 42-3

Sessions Details 42-6

Sub-session Details – NAC Details 42-8

Encryption Statistics 42-9

NAC Session Summary 42-10

Protocol Statistics 42-11

VLAN Mapping Sessions 42-12

Global IKE/IPSec Statistics 42-12

Crypto Statistics	42-13
Compression Statistics	42-13
Cluster Loads	42-14
SSO Statistics for Clientless SSL VPN Session	42-14

CHAPTER 43

Monitoring Routing 43-1

Monitoring OSPF LSAs	43-1
Type 1	43-1
Type 2	43-2
Type 3	43-3
Type 4	43-3
Type 5	43-4
Type 7	43-4
Monitoring OSPF Neighbors	43-5
Monitoring EIGRP Neighbors	43-7
Displaying Routes	43-8

CHAPTER 44

Monitoring Properties 44-1

Monitoring AAA Servers	44-1
Viewing AAA Server Statistics	44-1
Updating the Operational State of an AAA Server	44-2
Fields Used to Monitor AAA Servers	44-3
Monitoring Device Access	44-4
Monitoring User Lockouts	44-5
Viewing Lockouts	44-5
Removing All User Lockouts	44-6
Removing One User Lockout	44-7
Monitoring Authenticated Users	44-8
Monitoring Active Sessions	44-9
Viewing Active Sessions	44-9
Disconnecting an Active Session	44-11
Fields Used to Monitor Device Access	44-12
Fields for Monitoring User Lockouts	44-12
Fields for Monitoring Users Who Have Authenticated with a Server	44-13
Connection Graphs	44-13
Perfmon	44-13
Xlates	44-14
CRL	44-15

DNS Cache	44-15
IP Audit	44-16
System Resources Graphs	44-18
Blocks	44-19
CPU	44-19
Memory	44-20
WCCP	44-20
Service Groups	44-21
Redirection	44-21

CHAPTER 45

Monitoring Logging	45-1
About Log Viewing	45-1
Log Buffer	45-1
Log Buffer Viewer	45-2
Real-Time Log Viewer	45-3
Real-Time Log Viewer	45-3

CHAPTER 46

Monitoring Failover	46-1
Monitoring Failover in Single Context Mode or in a Security Context	46-1
Status	46-1
Graphs	46-4
Monitoring Failover in the System Execution Space	46-6
System	46-6
Failover Group 1 and Failover Group 2	46-9

CHAPTER 47

Monitoring Trend Micro Content Security	47-1
Threats	47-1
Live Security Events	47-2
Live Security Events Log	47-3
Software Updates	47-4
Resource Graphs	47-4
CSC CPU	47-4
CSC Memory	47-5

PART 6**Reference****APPENDIX A**

Feature Licenses and Specifications	A-1
Security Appliance and ASDM Release Compatibility	A-1

Client PC Operating System and Browser Requirements	A-1
Supported Platforms and Feature Licenses	A-2
Security Services Module Support	A-9
VPN Specifications	A-10

APPENDIX B

Troubleshooting B-1

Testing Your Configuration	B-1
Enabling ICMP Debug Messages and System Log Messages	B-1
Pinging Security Appliance Interfaces	B-2
Pinging Through the Security Appliance	B-4
Disabling the Test Configuration	B-5
Traceroute	B-6
Packet Tracer	B-6
Reloading the Security Appliance	B-6
Recovering from a Lockout	B-6
Performing Password Recovery	B-7
Recovering Passwords for the ASA 5500 Series Adaptive Security Appliance	B-7
Recovering Passwords for the PIX 500 Series Security Appliance	B-8
Disabling Password Recovery	B-9
Using the ROM Monitor to Load a Software Image	B-10
Erasing the Flash File System	B-11
Other Troubleshooting Tools	B-12
Viewing Debug Messages	B-12
Capturing Packets	B-12
Viewing the Crash Dump	B-12
TACACS+ Server Lockout	B-12
Verifying that Server Authentication and Authorization are Working	B-12
User's Identity not Preserved Across Contexts	B-13
Common Problems	B-13

APPENDIX C

Configuring an External Server for Authorization and Authentication C-1

Selecting LDAP, RADIUS, or Local Authentication and Authorization	C-1
Understanding Policy Enforcement of Permissions and Attributes	C-2
Configuring an External LDAP Server	C-2
Reviewing the LDAP Directory Structure and Configuration Procedure	C-3
Organizing the Security Appliance LDAP Schema	C-3
Searching the Hierarchy	C-4
Binding the Security Appliance to the LDAP Server	C-5

Defining the Security Appliance LDAP Schema	C-5
Cisco-AV-Pair Attribute Syntax	C-14
Example Security Appliance Authorization Schema	C-15
Loading the Schema in the LDAP Server	C-18
Defining User Permissions	C-18
Example User File	C-18
Configuring an External RADIUS Server	C-19
Reviewing the RADIUS Configuration Procedure	C-19
Security Appliance RADIUS Authorization Attributes	C-19
Security Appliance TACACS+ Attributes	C-26

INDEX



Preface

The *ASDM User Guide* contains the information that is available in the ASDM online help system.

This preface contains the following topics:

- [Related Documentation, page xxxix](#)
- [Document Conventions, page xxxix](#)
- [Obtaining Documentation and Submitting a Service Request, page xl](#)

Related Documentation

For more information, refer to the following documentation:

- *Release Notes for Cisco ASDM*
- *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide*
- *Cisco ASA 5580 Adaptive Security Appliance Command Reference*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5505 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5580 Adaptive Security Appliance System Log Messages*
- *Open Source Software Licenses for ASA and PIX Security Appliances*

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.

- Information you need to enter in examples is shown in **boldface screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

**Note**

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



PART 1

Getting Started



CHAPTER 1

Welcome to ASDM

Welcome to ASDM, a browser-based, Java applet that you use to configure and monitor the software on security appliances. ASDM is loaded by the adaptive security appliance, and enables you to configure, monitor, and manage the device.



Note

If you change the color scheme of your operating system while ASDM is running, you should restart ASDM, because some ASDM screens might not display correctly.

This section includes the following topics:

- [Multiple ASDM Session Support, page 1-1](#)
- [Caveats, page 1-1](#)
- [Unsupported Commands, page 1-2](#)
- [About the ASDM Interface, page 1-3](#)
- [About the Help Window, page 1-13](#)
- [Home Pane, page 1-14](#)
- [System Home Pane, page 1-21](#)

Multiple ASDM Session Support

ASDM allows multiple PCs or workstations to each have one browser session open with the same adaptive security appliance software. A single adaptive security appliance can support up to five concurrent ASDM sessions in single, routed mode. Only one session per browser per PC or workstation is supported for a specified adaptive security appliance. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a maximum of 32 total connections for each adaptive security appliance.

Caveats

Use the Bug Toolkit on Cisco.com to view current caveat information. You can access the Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Unsupported Commands

This section includes the following topics:

- [Ignored and View-Only Commands, page 1-2](#)
- [Effects of Unsupported Commands, page 1-3](#)

ASDM supports almost all commands available for the adaptive security appliance, but ASDM ignores some commands in an existing configuration. Most of these commands can remain in your configuration; see [Show Commands Ignored by ASDM on Device](#) for more information.

In addition, ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, do not use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Ignored and View-Only Commands

[Table 1-1](#) lists commands that ASDM supports in the configuration when added through the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Table 1-1 *List of Unsupported Commands*

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used
capture	Ignored
dns-guard	Ignored
eject	Unsupported
established	Ignored.
failover timeout	Ignored
icmp-unreachable rate-limit	Ignored
ipv6 , any IPv6 addresses	Ignored
pager	Ignored
pim accept-register route-map	Ignored. You can configure only the list option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored
service-policy global	Ignored if it uses a match access-list class. For example: <pre>access-list myacl line 1 extended permit ip any any class-map mycm match access-list mycl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>

Table 1-1 **List of Unsupported Commands (continued)**

Unsupported Commands	ASDM Behavior
<code>sysopt nodnsalias</code>	Ignored
<code>sysopt uauth allow-http-cache</code>	Ignored
<code>terminal</code>	Ignored
<code>threat-detection statistics tcp-intercept</code>	Ignored
<code>threat-detection scanning-threat shun duration</code>	Ignored
<code>switchport trunk native vlan</code>	Ignored

Effects of Unsupported Commands

If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but other configurations are available.

If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the list of unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.

If you load an existing running configuration that includes the **alias** command, ASDM enters Monitor-only mode. This mode allows you to access the following functions:

- The Monitoring area
- The CLI tool. To access the CLI tool, choose **Tools > Command Line Interface**.

To exit Monitor-only mode, use the CLI tool or access the adaptive security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.



Note

You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set as less than or equal to three by your system administrator. For more information, choose **Configuration > Properties > Device Administration > User Accounts** and **Configuration > Device Access > AAA Access**.

About the ASDM Interface

The ASDM interface is designed to provide easy access to the many features that the adaptive security appliance supports. The ASDM interface includes the following components:

- **Menu Bar**—Provides quick access to files, tools, wizards, and help. Many menu items also have keyboard shortcuts.
- **Toolbar**—Lets you navigate ASDM. From the toolbar you can access the home pane, configuration, and monitoring panes. You can also get help and navigate between panes.
- **Status Bar**—Shows the time, connection status, user, and privilege level.
- **Device List**—Displays a list of devices that you can access through ASDM. For more information, see [Device List, page 1-9](#).

- **Addresses/Services/Time Ranges**—Displays a dockable pane that shows various objects you can use in the rules tables when you create access, filter, and service rules.
- **Navigation**—Displays a dockable pane that lets you navigate the Configuration and Monitoring screens.

**Note**

Tool tips have been added for various parts of the GUI, including wizards, and the configuration and monitoring panes.

This section includes the following topics:

- [Menus, page 1-4](#)
- [Toolbar, page 1-7](#)
- [Status Bar, page 1-9](#)
- [Common Buttons, page 1-10](#)
- [Keyboard Shortcuts, page 1-11](#)
- [Enabling Extended Screen Reader Support, page 1-12](#)

Menus

You can access the ASDM menus using the mouse or keyboard. See [Keyboard Shortcuts, page 1-11](#) for more information about accessing the menu bar from the keyboard. ASDM has the following menus:

- [File Menu, page 1-4](#)
- [View Menu, page 1-5](#)
- [Tools Menu, page 1-6](#)
- [Wizards Menu, page 1-6](#)
- [Window Menu, page 1-7](#)
- [Help Menu](#)

File Menu

The File menu manages adaptive security appliance configurations, and includes the following items:

- **Refresh ASDM with the Running Configuration on the Device**—Loads a copy of the running configuration to ASDM. Click **Refresh** to make sure ASDM has a current copy of the running configuration.
- **Reset Device to the Factory Default Configuration**—Restores the configuration to the factory default. See the [Reset Device to the Factory Default Configuration](#) dialog box for more information.
- **Show Running Configuration in New Window**—Displays the current running configuration in a new window.
- **Save Running Configuration to Flash**—Writes a copy of the running configuration to Flash memory.
- **Save Running Configuration to TFTP Server**—Stores a copy of the current running configuration file on a TFTP server. See the [Save Running Configuration to TFTP Server](#) dialog box for more information.

- **Save Running Configuration to Standby Unit**—Sends a copy of the running configuration file on the primary unit to the running configuration of a failover standby unit.
- **Save Internal Log Buffer to Flash**—Saves the internal log buffer to Flash memory.
- **Print**—Prints the current page. We recommend landscape page orientation when you print rules. When you use Internet Explorer, permission to print is already granted when you originally accepted the signed applet.
- **Clear ASDM Cache**—Removes local ASDM images. ASDM downloads images locally when you connect to ASDM.
- **Clear Internal Log Buffer**—Empties the system log message buffer.
- **Exit**—Closes ASDM.

View Menu

The View menu lets you display various parts of the ASDM interface. Certain items are dependent on the current view. You cannot select items that cannot be displayed in the current view. For example, the Latest ASDM Syslog Messages pane is only available when the home view is displayed.

- **Home**—Displays the home view.
- **Configuration**—Displays the configuration view.
- **Monitoring**—Displays the monitoring view.
- **Device List**—Displays a list of devices in a dockable pane. For more information, see [Device List, page 1-9](#).
- **Navigation**—Shows and hides the display of the Navigation pane in the configuration and monitoring views.
- **Latest ASDM Syslog Messages**—Shows and hides the display of the Latest ASDM Syslog Messages pane in the home view.
- **Addresses**—Shows and hides the display of the Addresses pane. The Addresses pane is only available for the Access Rules, NAT Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- **Services**—Shows and hides the display of the Services pane. The Services pane is only available for the Access Rules, NAT Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- **Time Ranges**—Shows and hides the display of the Time Ranges pane. The Time Ranges pane is only available for the Access Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- **Global Pools**—Shows and hides the display of the Global Pools pane. The Global Pools pane is only available for the NAT Rules pane in the configuration view.
- **Find**—Locates an item for which you are searching, such as a feature or the ASDM Assistant.
- **Back**—See [Common Buttons](#) for more information.
- **Forward**—See [Common Buttons](#) for more information.
- **Reset Layout**—Returns the layout to the default configuration.
- **Office Look and Feel**—Changes the screen fonts and colors to the Microsoft Office settings.

Tools Menu

The Tools menu provides you with the following series of tools to use with ASDM:

- **Command Line Interface**—Provides a text-based tool for sending commands to the adaptive security appliance and viewing the results. See the [Command Line Interface](#) dialog box for more information.
- **Show Commands Ignored by ASDM on Device**—Displays unsupported commands that have been ignored by ASDM. See the [Show Commands Ignored by ASDM on Device](#) dialog box for more information.
- **Packet Tracer**—Lets you trace a packet from a specified source address and interface to a destination. You can specify the protocol and port of any type of data and view the lifespan of a packet, with detailed information about actions taken on it. See the [Packet Tracer](#) dialog box for more information.
- **Ping**—Lets you verify the configuration and operation of the adaptive security appliance and surrounding communications links, as well as perform basic testing of other network devices. See the [Ping](#) dialog box for more information.
- **Traceroute**—Lets you determine the route packets will take to their destination. See the [Traceroute](#) dialog box for more information.
- **File Management**—Lets you view, move, copy, and delete files stored in Flash memory. You can also create a directory in Flash memory. See the [File Management](#) dialog box for more information. You can also display the [File Transfer](#) dialog box to transfer files between various file systems, including TFTP, Flash memory, and your local PC.
- **Upgrade Software from Local Computer**—Lets you choose an adaptive security appliance image, ASDM image, or another image on your PC, and upload the file to Flash memory. See the [Upgrade Software from Local Computer](#) dialog box for more information.
- **Upgrade Software from Cisco.com**—Lets you upgrade adaptive security appliance software and ASDM software through a wizard. See the [Upgrade Software from Cisco.com Wizard](#) for more information.
- **Upload ASDM Assistant Guide**—Lets you upload an XML file to Flash memory that contains information used in the ASDM Assistant. You can download these files from Cisco.com. See the [ASDM Assistant](#) dialog box for more information.
- **System Reload**—Lets you restart the ASDM and reload the saved configuration into memory. See the [System Reload](#) dialog box for more information.
- **Administrator's Alerts to Clientless SSL VPN Users**—Lets an administrator send an alert message to clientless SSL VPN users. See the [Administrator's Alert to Clientless SSL VPN Users](#) dialog box for more information.
- **Preferences**—Changes the behavior of specified ASDM functions between sessions. See the [Preferences](#) dialog box for more information.
- **ASDM Java Console**—Shows the Java console. See the [ASDM Java Console](#) dialog box for more information.

Wizards Menu

The Wizards menu lets you run a wizard to configure multiple features.

- **Startup Wizard**—This wizard walks you, step-by-step, through the initial configuration of your adaptive security appliance. For more information, see [Using the Startup Wizard](#).

- IPsec VPN Wizard—This wizard enables you to configure an IPsec VPN policy on your adaptive security appliance. For more information, see the [VPN Wizard](#).
- SSL VPN Wizard—This wizard enables you to configure an SSL VPN policy on your adaptive security appliance. For more information, see the [VPN Wizard](#).
- High Availability and Scalability Wizard— This wizard allows you to configure failover on your adaptive security appliance. For more information, see [High Availability](#).
- Packet Capture Wizard— This wizard allows you to configure packet capture on your adaptive security appliance. The wizard runs one packet capture on each ingress and egress interface. After you run the capture, you can save the capture on your computer, and then examine and analyze the capture with a packet analyzer. For more information, see the [Packet Capture Wizard](#).

Window Menu

The Window menu enables you to move between ASDM windows. The active window appears as the selected window.

Help Menu

The Help menu provides links to online Help, as well as information about ASDM and the adaptive security appliance.

- Help Topics—Opens a new browser window with help organized by contents, screen name, and indexed in the left frame. Use these methods to find help for any topic, or search using the Search tab.
- Help for Current Screen—Opens context-sensitive help about that screen. The wizard runs the screen, pane, or dialog box that is currently open. You can also click the question mark (?) help icon for context-sensitive help.
- Release Notes—Opens the most current version of the *Cisco ASDM Release Notes* on Cisco.com. The Release Notes contain the most current information about ASDM software and hardware requirements, and the most current information about changes in the software.
- Getting Started—Opens the Getting Started help topic to help you begin using ASDM.
- ASDM Assistant—Opens the ASDM Assistant, which lets you search downloadable content from Cisco.com, with details about performing certain tasks.
- About Cisco Adaptive Security Appliance (ASA)—Displays information about the adaptive security appliance, including the software version, hardware set, configuration file loaded at startup, and software image loaded at startup. This information is helpful in troubleshooting.
- About Cisco ASDM 6.1—Displays information about ASDM such as the software version, hostname, privilege level, operating system, device type, and Java version.

Toolbar

The Toolbar below the menus provides access to the home view, configuration view, and monitoring view. It also lets you choose between the system and security contexts in multiple context mode, and provides navigation and other commonly used functions.

- **System/Contexts**—Click the down arrow to open the context list in a left-hand pane, and click the up arrow to restore the context drop-down list. After you have expanded this list, click the left arrow to collapse the pane, and the right arrow to restore the pane. To manage the system, choose **System** from the list. To manage a context, choose one from the list.
- **Home**—Displays the [Home Pane](#), which lets you view important information about your adaptive security appliance such as the status of your interfaces, the version you are running, licensing information, and performance. See the Home pane for more information. In multiple mode, the system does not have a Home pane.
- **Configuration**—Configures the adaptive security appliance. Choose a feature button in the left-hand pane to configure that feature.
- **Monitoring**—Monitors the adaptive security appliance. Choose a feature button in the left-hand pane to monitor that feature.
- **Back**—Takes you back to the last pane of ASDM you visited.
- **Forward**—Takes you forward to the last pane of ASDM you visited.
- **Search**—Lets you search for a feature in ASDM. The Search function looks through the titles of each pane and presents you with a list of matches, and gives you a hyperlink directly to that pane. If you need to switch quickly between two different panes you found, click **Back** or **Forward**. See the [ASDM Assistant](#) for more information.
- **Refresh**—Refreshes ASDM with the current running configuration, except for graphs in any of the monitoring graphs.
- **Save**—Saves the running configuration to the startup configuration for write-accessible contexts only.
- **Help**—Shows context-sensitive help for the screen that is currently open.

ASDM Assistant

The ASDM Assistant dialog box lets you search for useful ASDM procedural help about certain tasks. You must first upload the ASDM Assistant Guide through the Tools menu to make the help available. See the [ASDM Assistant](#) dialog box for more information.

This dialog box provides a two-pane window that lets you enter queries on the left-hand pane, lists the available links to information that result from those queries, and then displays the information that you selected or additional links on the right-hand pane.

The How Do I? tab lets you select specific areas on which to search. The Search tab lets you enter terms and features about which you want more information and specify the type of results you want.

How Do I? Tab

Fields

- **Show tasks**—Choose the type of information you want from the drop-down list. The available types are Security Policy, ASDM, Administration, and All.

Search Tab

Fields

- **For**—Enter the term about which you want more information.

- How Do I?—Check this check box to include downloadable content from Cisco.com, with details about performing certain tasks.
- Features—Check to include features about which you want more details.
- Include—Select from the following options the information you want to include: Exact Phrase, Any Word, or All Words.
- Exclude—Specify the information that you want to exclude.
- Search—Click to start the query.

Status Bar

The status bar appears at the bottom of the ASDM window, and shows the following areas from left to right.

- Status—Shows the status of the configuration (for example, “Device configuration loaded successfully.”).
- User Name—Shows the username of the ASDM user. If you logged in without a username, the username is “admin.”
- User Privilege—Shows the privilege of the ASDM user.
- Commands Ignored by ASDM—Click the icon to show a list of commands from your configuration that ASDM did not process. These commands will not be removed from the configuration. See [Show Commands Ignored by ASDM on Device](#) for more information.
- Status of Connection to Device—Shows the ASDM connection status to the adaptive security appliance. See [Connection to Device](#) for more information.
- Save to Flash Needed—Shows that you made configuration changes in ASDM, but that you still must save the running configuration to the startup configuration.
- Refresh Needed—Shows that you need to refresh the configuration from the adaptive security appliance to ASDM, because the configuration on the adaptive security appliance changed (for example, you made a change to the configuration through the CLI).
- SSL Secure—Shows that the connection to ASDM is secure because it uses SSL.
- Time—Shows the time that is set on the switch that contains the adaptive security appliance.

Connection to Device

ASDM maintains a constant connection to the adaptive security appliance to maintain up-to-date monitoring and home pane data. This dialog box shows the status of the connection. When you make a configuration change, ASDM opens a second connection for the duration of the configuration, and then closes it; however, this dialog box does not represent the second connection.

Device List

The device list is a dockable pane. You can click one of the three buttons in the header to maximize or restore this pane, make it a floating pane that you can move, hide the pane, or close the pane. This pane is available in the home, configuration, monitoring, and system views. You can use this pane to switch to another device; however, that device must run the same version of ASDM that you are currently running. To display the pane fully, you must have at least two devices listed.

**Note**

You cannot switch to another device that runs a different version of ASDM.

To use this pane to connect to another device, perform the following steps:

-
- Step 1** Click **Add** to add another device to the list.
The Add Device dialog box appears.
- Step 2** In the Device/IP Address/Name field, type the device name or IP address of the device, and then click **OK**.
- Step 3** Click **Delete** to remove a selected device from the list.
- Step 4** Click **Connect** to connect to another device.
The Enter Network Password dialog box appears.
- Step 5** Type your username and password in the applicable fields, and then click **Login**.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Common Buttons

These buttons appear on many ASDM panes:

- **Apply**—Sends changes made in ASDM to the adaptive security appliance and applies them to the running configuration.
- **Save** —Writes a copy of the running configuration to Flash memory.
- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After you click **Reset**, click **Refresh** to make sure that information from the current running configuration is displayed.
- **Restore Default**—Clears the selected settings and returns to the default settings.
- **Cancel**—Discards changes and returns to the previous pane.
- **Enable**—Displays read-only statistics for a feature.
- **Close**—Closes an open dialog box.
- **Clear**—Removes information from a field or box, or removes a check from a check box.
- **Back**—Returns you to the previous pane.
- **Forward**—Takes you to the next pane.
- **Help**—Displays help for the selected pane.

Keyboard Shortcuts

You can use the keyboard to navigate the ASDM interface.

Table 1-2 lists the keyboard shortcuts you can use to move across the three main areas of the ASDM interface.

Table 1-2 Navigating ASDM

To display the	Windows/Linux	MacOS
Home Page	Ctrl+H	Shift+Command+H
Configuration Page	Ctrl+G	Shift+Command+G
Monitoring Page	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+Left Arrow	Command+[
Forward	Alt+Rightarrow	Command+]
Refresh the display	F5	Command+R
Cut	Ctrl+X	Command+X
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
Save the configuration	Ctrl+S	Command+S
Popup menus	Shift+F10	—
Close a secondary window	Alt+F4	Command+W
Find	Ctrl+F	Command+F
Exit	Alt+F4	Command+Q
Exit a table or text area	Ctrl_Shift or Ctrl+Shift+Tab	Ctrl+Shift or Ctrl+Shift+Tab

Table 1-3 lists the keyboard shortcut you can use to navigate within a pane.

Table 1-3 Moving the Focus

To move the focus to the	Press
next field	Tab
previous field	Shift+Tab
next field when the focus is in a table	Ctrl+Tab
previous field when the focus is in a table	Shift+Ctrl+Tab
next tab (when a tab has the focus)	Right Arrow
previous tab (when a tab has the focus)	Left Arrow
next cell in a table	Tab
previous sell in a table	Shift+Tab
next pane (when multiple panes are displayed)	F6
previous pane (when multiple panes are displayed)	Shift+F6

Table 1-4 lists the keyboard shortcuts you can use with the Log Viewers.

Table 1-4 Log Viewer Keyboard Shortcuts

To display the	Windows/Linux	MacOS
Pause and Resume Real-Time Log Viewer	Ctrl+U	Command+.
Refresh Log Buffer Window	F5	Command+R
Clear Internal Log Buffer	Ctrl+Delete	Command+Delete
Copy Selected Log Entry	Ctrl+C	Command+C
Save Log	Ctrl+S	Command+S
Print	Ctrl+P	Command+P
Close a secondary window	Alt+F4	Command+W

Table 1-5 lists the keyboard shortcuts you can use to access menu items.

Table 1-5 Log Viewer Keyboard Shortcuts

To access the	Windows/Linux
Menu Bar	Alt
Next Menu	Right Arrow
Previous Menu	Left Arrow
Next Menu Option	Down Arrow
Previous Menu Option	Up Arrow
Selected Menu Option	Enter

Enabling Extended Screen Reader Support

By default, labels and descriptions are not included in tab order when you press the Tab key to navigate a pane. Some screen readers, such as JAWS, only read screen objects that have the focus. You can include the labels and descriptions in the tab order by enabling extended screen reader support.

To enable extended screen reader support, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
The Preferences dialog box appears.
 - Step 2** On the General tab, check the **Enable screen reader support** check box.
 - Step 3** Click **OK**.
 - Step 4** Restart ASDM to activate screen reader support.
-

Organizational Folder

Some nodes in the navigation tree for the configuration and monitoring screens do not have associated configuration or monitoring panes. They are used to organize related configuration and monitoring items. Clicking on these folders displays a list of sub-items in the right-hand pane. You can click the name of a sub-item to go to that item.

About the Help Window

This section includes the following topics:

- [Header Buttons, page 1-13](#)
- [Browser Window, page 1-13](#)

Header Buttons

Click the applicable button to obtain the information you need.

- **About ASDM**—Displays information about ASDM, including the hostname, version number, device type, adaptive security appliance software version number, privilege level, username, and operating system being used.
- **Search**—Searches for information among online help topics.
- **Using Help**—Describes the most efficient methods for using online help.
- **Glossary**—Lists terms found in ASDM and adaptive security appliance devices.
- **Left-Pane Links**—Moves through online help topics.
- **Contents**—Displays a table of contents.
- **Screens**—Lists help files by screen name.
- **Index**—Provides an index of help topics found in ASDM online help.
- **Right-Pane Help Content**—Displays the help for the selected topic.

Browser Window

When you open help and a help page is already open, the new help page will appear in the same browser window. If no help page is open, then the help page will appear in a new browser window.

When you open help and Netscape Communicator is the default browser, the help page will appear in a new browser window. If Internet Explorer is the default browser, the help page may appear either in the last-visited browser window or in a new browser window, according to your browser settings. You can control this behavior in Internet Explorer by choosing **Tools > Internet Options > Advanced > Reuse windows for launching shortcuts**.

Home Pane

The ASDM home pane lets you view important information about your adaptive security appliance. Status information on the home pane is updated every ten seconds. This pane usually has two tabs: Device Dashboard and Firewall Dashboard.

If you have a CSC SSM installed in your adaptive security appliance, the Content Security tab also appears on the home pane. The additional tab displays status information about the CSC SSM software.

If you have IPS software installed in your adaptive security appliance, the Intrusion Prevention tab also appears on the home pane. The additional tab displays status information about the IPS software.

This section includes the following topics:

- [Device Dashboard Tab, page 1-15](#)
- [Firewall Dashboard Tab, page 1-17](#)
- [Content Security Tab, page 1-18](#)
- [Intrusion Prevention Tab, page 1-20](#)

Fields

- Latest ASDM Syslog Messages—Shows the most recent system messages generated by the adaptive security appliance, up to a maximum of 100 messages.

Click the square icon in the header to expand the logging pane. Click the double square icon in the header to return to the default size. Drag the divider up or down to resize the pane. You can also right-click an event and choose **Clear Content**, to clear the current messages; **Save Content**, to save the current messages to a file on your PC, **Copy**, to copy the content; and **Color Settings**, to change the background and foreground colors of system messages according to their severity. Click one of the four buttons in the header on the right-hand side to maximize or restore the pane, make it a floating pane that you can move, hide the pane, or close the pane.

- Enable Logging—Click to enable logging and display system log messages.
- Stop message display—Click the red icon on the right-hand side to stop updating the display of system log messages.
- Resume message display—Click the green icon on the right-hand side to continue updating the display of system log messages.
- Configure ASDM Syslog Filters—Click the filters icon on the right-hand side to open the [Logging Filters](#) pane.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Device Dashboard Tab

The Device Dashboard tab lets you view, at a glance, important information about your adaptive security appliance, such as the status of your interfaces, the version you are running, licensing information, and performance.

Fields

- Device Information—Includes two tabs to show device information.
 - General—Shows the following information:
 - Host Name—*Display only*. Shows the adaptive security appliance hostname. See [Device Name/Password](#) to set the hostname.
 - ASA Version—*Display only*. Shows the adaptive security appliance software version.
 - Device Uptime—*Display only*. Shows how long the adaptive security appliance has been running.
 - ASDM Version—*Display only*. Shows the ASDM version.
 - Device Type—*Display only*. Shows the adaptive security appliance model.
 - Firewall Mode—*Display only*. Shows the firewall mode, either Routed or Transparent. See [Firewall Mode Overview](#) for more information.
 - Total Flash—*Display only*. Shows the total amount of available Flash memory.
 - Context Mode—*Display only*. Shows the context mode, either Single or Multiple. See [Security Context Overview](#) for more information.
 - Total Memory—*Display only*. Shows the total amount of available RAM.
 - License—*Display only*. Shows the level of support for licensed features on the adaptive security appliance. Shows the following information:
 - License—*Display only*. Shows the type of license, either Base or Premium.
 - Number of days until a time-based license expires, if applicable.
 - Inside Hosts—*Display only*. Shows inside hosts (ASA 5505 only).
 - Max VLANs—*Display only*. Shows the maximum number of VLANs allowed.
 - Failover—*Display only*. Shows the failover configuration, either Active/Active or Active/Standby.
 - Security Contexts—*Display only*. Shows the maximum numbers of security contexts allowed.
 - Dual ISP Support—*Display only*. Shows dual ISP support, if enabled (ASA 5505 only).
 - GTP/GPRS—*Display only*. Shows whether GTP/GPRS is enabled or disabled.
 - Encryption—*Display only*. Shows the type of encryption enabled.
 - VPN Peers—*Display only*. Shows the number of VPN peers allowed. This entry is blank if no VPN peers are supported.
 - Clientless SSL VPN Peers—*Display only*. Shows the number of clientless SSL VPN peers allowed.
- VPN Tunnels Status—Routed, single mode only. Shows the following information:
 - IKE—*Display only*. Shows the number of connected IKE tunnels.
 - IPSec—*Display only*. Shows the number of connected IPSec tunnels.

- Clientless SSL VPN—*Display only*. Shows the number of clientless, connected SSL VPN tunnels.
 - SSL VPN Client—*Display only*. Shows the number of connected SSL VPN client tunnels.
- System Resources Status—Shows the following CPU and memory usage statistics:
 - CPU—*Display only*. Shows the current percentage of CPU being used.
 - CPU Usage (percent)—*Display only*. Shows the CPU usage for the last five minutes.
 - Memory—*Display only*. Shows the current amount of memory being used in MB.
 - Memory Usage (MB)—*Display only*. Shows the memory usage for the last five minutes in MB.
- Interface Status—Shows the status of each interface. If you select an interface row, the input and output throughput in Kbps shows under the table.
 - Interface—*Display only*. Shows the interface name.
 - IP Address/Mask—*Display only*. Routed mode only. Shows the IP address and subnet mask of the interface.
 - Line—*Display only*. Shows the administrative status of the interface. A red icon is displayed if the line is down, and a green icon is displayed if the line is up.
 - Link—*Display only*. Shows the link status of the interface. A red icon is displayed if the link is down, and a green icon is displayed if the link is up.
 - Kbps—*Display only*. Shows the current number of throughput in Kbps that cross the interface.
- Traffic Status—Shows graphs for connections per second for all interfaces and for the traffic throughput of the lowest security interface.
 - Connections per Second Usage—*Display only*. Shows the UDP and TCP connections per second during the last five minutes. This graph also shows the current number of connections by type, UDP, TCP, and the total.
 - Name Interface Traffic Usage (Kbps)—*Display only*. Shows the traffic throughput for the lowest security interface. If you have multiple interfaces at the same level, then ASDM shows the first interface alphabetically. This graph also shows the current throughput by type, input Kbps, and output Kbps.
- Latest ASDM Syslog Messages—Shows the latest system messages generated by the adaptive security appliance.
 - Stop Message Display—Stops logging to ASDM.
 - Resume Message Display—Continues logging to ASDM.
 - Configure ASDM Filters—Configures logging filters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Firewall Dashboard Tab

The Firewall Dashboard tab lets you view important information about the traffic passing through your security appliance, including the number of connections, NAT translations, dropped packets, attacks, and top usage statistics.

The Traffic Overview statistics are enabled by default. If you disable basic threat detection (see the [“Configuring Basic Threat Detection” section on page 27-1](#)), then this tab includes an Enable button that lets you enable basic threat detection.

The Top 10 Access Rules are also enabled by default. If you disable threat detection statistics for access rules (see the [“Configuring Threat Statistics” section on page 27-4](#)), then this tab includes an Enable button that lets you enable statistics for access rules.

The Top Usage Status statistics are disabled by default. This tab includes Enable buttons that let you enable the features, or you can enable them according to the [“Configuring Threat Statistics” section on page 27-4](#). The Top 10 Services Enable button enables statistics for both ports and protocols (both must be enabled for the display). The Top 10 Sources and Top 10 Destinations Enable buttons enable statistics for hosts.



Caution

Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. Enabling statistics for hosts affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Enabling statistics for ports, however, has modest impact.

Fields

- Traffic Overview—*Display only*. Shows runtime statistics, including the number of connections, NAT translations, and dropped packets.
 - Connection Statistics—*Display only*. Shows the number of connections and NAT translations.
 - Dropped Packets Rate—*Display only*. Shows the rate of dropped packets per second caused by access list denials and application inspections.
 - Possible Scan and SYN Attack Rates—*Display only*. Shows the rate of dropped packets per second that are identified as part of a scanning attack, or that are incomplete sessions detected, such as TCP SYN attack detected or no data UDP session attack detected.
- Top 10 Access Rules—*Display only*. Shows the most active access rules.
 - Interval—Lets you view information based on the interval you choose. Available values are Last 1 hour, Last 8 hours, and Last 24 hours.
 - Based on—*Display only*. Shows that this statistic shows number of packet hits only.
 - Display—Lets you view the same information in three different formats: Table, Pie, or Bar.
 - Interface—Shows the interface to which the rule is applied.
 - Rule#—Shows the rule number used.
 - Hits—Shows the number of packet hits that occurred.
 - Source—Shows the source IP address.
 - Dest—Shows the destination IP address.
 - Service—Shows the service (protocol or port) for the connection.
 - Action—Shows whether the rule is a permit or deny rule.

In the Table view, you can select a rule in the list and right-click the rule to display a popup menu item, **Show Rule**. Choose this item to go to the Access Rules table and select that rule in this table.

- Top Usage Status—Provides usage status for hosts (source and destinations), and ports and protocols.
 - Interval—Lets you view information based on the interval you choose. Available values are Last 1 hour, Last 8 hours, and Last 24 hours.
 - Based On—Shows the statistics in Packet Hits or Bytes.
 - Display—Lets you view the same information in three different formats: Table, Pie, or Bar.
 - Top 10 Services—Shows statistics for the top 10 services, including the combined statistics of TCP/UDP port and IP protocol types.
 - Top 10 Sources—Shows the top 10 host source addresses.
 - Top 10 Destinations—Shows the top 10 host destination addresses.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Content Security Tab

The Content Security tab lets you view important information about the Content Security and Control (CSC) SSM. This pane appears only if a CSC SSM is installed in the adaptive security appliance.

For an introduction to the CSC SSM, see [About the CSC SSM](#).



Note

If you have not completed the CSC Setup Wizard by choosing **Configuration > Trend Micro Content Security > CSC Setup**, you cannot access the panes under Home > Content Security. Instead, a dialog box appears and lets you access the Setup Wizard directly from this location.

Fields

- Device Information—Shows the following details:
 - Model—*Display only*. Shows the type of SSM installed in your adaptive security appliance.
 - Mgmt IP—*Display only*. Shows the IP address of the management interface for the CSC SSM.
 - Version—*Display only*. Shows the CSC SSM software version.
 - Last Update—*Display only*. Shows the date of the last software update obtained from Trend Micro.
 - Daily Node #—*Display only*. Shows the number of network devices for which the CSC SSM provided services in the preceding 24 hours. ASDM updates this field at midnight.

- Base License—*Display only*. Shows the license status for basic features of the CSC SSM, such as anti-virus, anti-spyware, and FTP file blocking. The license expiration date appears. If the license has expired, the expiration date appears. If no license is configured, the field shows “Not Available.”
- Plus License—*Display only*. Shows the license status for advanced features of the CSC SSM, such as anti-spam, anti-phishing, e-mail content filtering, and URL blocking and filtering. The license expiration date appears. If the license has expired, the expiration date appears. If no license is configured, the field shows “Not Available.”
- Licensed Nodes—*Display only*. Shows the maximum number of network devices for which your CSC SSM is licensed to provide services.
- System Resources Status—Shows the following CPU and memory usage statistics for the CSC SSM:
 - CPU—*Display only*. Shows the current percentage of CPU being used.
 - CSC SSM CPU Usage (percent)—*Display only*. Shows the CPU usage for the last five minutes.
 - Memory—*Display only*. Shows the current amount of memory being used in MB.
 - CSC SSM Memory Usage (MB)—*Display only*. Shows the memory usage for the last five minutes in MB.
- Threat Summary—Shows aggregated data about threats detected by the CSC SSM.
 - Threat Type—*Display only*. Lists five threat types: Virus, Spyware, URL Blocked, URL Filtered, and Spam.
 - Today—*Display only*. Shows the number of threats detected for each threat type in the past 24 hours.
 - Last 7 Days—*Display only*. Shows the number of threats detected for each threat type in the past seven days.
 - Last 30 Days—*Display only*. Shows the number of threats detected for each threat type within the past 30 days.
- Email Scan—Shows graphs for scanned e-mails and e-mail virus and spyware detected.
 - Email Scanned Count—*Display only*. Shows the number of e-mails scanned as separate graphs by e-mail protocol (SMTP or POP3), and as a combined graph for both supported e-mail protocols. The graphs display data in ten-second intervals.
 - Email Virus and Spyware—*Display only*. Shows the number of viruses and e-mails detected in e-mail scans as separate graphs by threat type (virus or spyware). The graphs display data in ten-second intervals.
- Latest CSC Security Events—Shows in real-time the security event messages received from the CSC SSM.
 - Time—*Display only*. Shows the time that an event occurred.
 - Source—*Display only*. Shows the IP address or hostname from which the threat came.
 - Threat/Filter—*Display only*. Shows the type of threat or, in the case of a URL filter event, the filter that triggered the event.
 - Subject/File/URL—*Display only*. Shows the subject of e-mails that contain a threat, the names of FTP files that contain a threat, or blocked or filtered URLs.
 - Receiver/Host—*Display only*. Shows the recipient of e-mails that contain a threat or the IP address or hostname of a threatened node.
 - Sender—*Display only*. Shows the source of e-mails that contain a threat.

- Content Action—*Display only*. Shows the action that is taken on the message or file content, such as delivering the content unaltered, deleting attachments, or cleaning attachments before delivering them.
- Msg Action—*Display only*. Shows the action that is taken on the message, such as delivering the message unchanged, delivering the message after deleting attachments, or not delivering the message.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Intrusion Prevention Tab

The Intrusion Prevention tab lets you view important information about IPS. This tab appears only when you have IPS software running on the AIP SSM that is installed on the adaptive security appliance.

For more information about intrusion prevention, see [Configuring IPS](#).

Connecting to IPS

To connect to the IPS software on the AIP SSM, perform the following steps:

-
- Step 1** From the main ASDM application window, click the **Intrusion Prevention** tab.
- Step 2** In the Connecting to IPS dialog box, choose one of the following options:
- Management IP Address—Connects to the IP address of the management port on the SSM.
 - Other IP Address or Hostname—Connects to an alternate IP address or hostname on the SSM.
- Step 3** Enter the port number in the Port field, and then click **Continue**.
- Step 4** In the Enter Network Password dialog box, type your username and password in the applicable fields, and then click **Login**.
-

Fields

- Device Information—Shows the following information:
 - Host Name—*Display only*. Shows the IPS hostname.
 - IPS Version—*Display only*. Shows the IPS software version.
 - IDM Version—*Display only*. Shows the IDM software version.
 - Bypass Mode—*Display only*. Shows the bypass mode, which can be set to On or Off.
 - Missed Packets Percentage—*Display only*. Shows the percentage of missed packets.
 - IP Address—*Display only*. Shows the IP address of the adaptive security appliance.

- Device Type—*Display only*. Shows the type and model of the adaptive security appliance.
- Total Data Storage—*Display only*. Shows the total amount of available data storage in MB.
- Total Sensing Interface—*Display only*. Shows the total number of sensing interfaces.
- System Resources Status—Shows the following CPU and memory usage statistics for the IPS software:
 - *Display only*. Percentage of CPU resources currently being used.
 - *Display only*. Average percentage of CPU resources being used.
 - *Display only*. Amount of memory currently being used.
 - *Display only*. Average amount of memory being used.
 - *Display only*. Amount of free memory and total memory available.
- Interface Status—Shows the following information:
 - Interface—*Display only*. Shows the type of interface to which you are connected. Choose an interface to view the sent and received packet counts.
 - Link—*Display only*. Shows the link status, which can be Up or Down.
 - Enabled—*Display only*. Shows the current connection status, which can be Yes (Enabled) or No (Not Enabled).
 - Speed—*Display only*. Shows the current connection speed.
 - Mode—*Display only*. Shows the current mode, which can be Management or Paired.
- Alert Summary—*Display only*. Lists the alerts, with assigned values of High, Med, Low, and Info, and the assigned threat rating.
- Alert Profile—*Display only*. Shows the alerts received in a color-coded graph, with assigned values of High (red), Med (yellow), Low (green), and Info (blue), and the assigned threat rating (magenta).
- Auto-Refresh every 10 seconds—Check this check box to refresh the current pane automatically every ten seconds.
- Refresh Page—Click to refresh the currently open pane manually.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Home Pane

The ASDM system home pane lets you view important status information about your adaptive security appliance. Many of the details available on the ASDM system home pane are available elsewhere in ASDM, but this pane shows at-a-glance how your adaptive security appliance is running. Status information on the system home pane is updated every ten seconds.

**Note**

This pane is available only in the security context.

Fields

- **Device List**—Displays the list of devices to which you can connect. For more information, see [Device List, page 1-9](#).
- **Interface Status**—Shows the following information:
 - **Interface**—*Display only*. Shows the type of interface to which you are connected. Choose an interface to view the total amount of traffic through the interface.
 - **Contexts**—*Display only*. Shows the current contexts of users (for example, admin).
 - **Line**—*Display only*. Shows the line status, which can be Up or Down.
 - **Link**—*Display only*. Shows the link status, which can be Up or Down.
 - **Kbps**—*Display only*. Shows the current connection speed in kilobits per second.
- **CPU Status**—Shows the following CPU and context usage statistics:
 - **Total Usage tab**—*Display only*. Shows the total percentage of CPU usage and the total percentage of CPU usage history in seconds.
 - **Context Usage tab**—*Display only*. Shows the total percentage of context usage in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.
- **Connection Status**—Shows the following connection usage and context connection usage statistics:
 - **Total Connections tab**—*Display only*. Shows the total number of connections.
 - **Context Connections tab**—*Display only*. Shows the total number of context connections in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.
- **Memory Status**—Shows the following CPU and context usage statistics:
 - **Total Usage tab**—*Display only*. Shows the total amount of memory usage in MB and the total amount of memory usage history in MB.
 - **Context Usage tab**—*Display only*. Shows the total amount of memory usage in various contexts in MB in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•



CHAPTER 2

Introduction to the Security Appliance

The security appliance combines advanced stateful firewall and VPN concentrator functionality in one device, and for some models, an integrated intrusion prevention module called the AIP SSM or an integrated content security and control module called the CSC SSM. The security appliance includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPSec and clientless SSL support, and many more features. See [Appendix A, “Feature Licenses and Specifications,”](#) for a list of supported platforms and features. For a list of new features, see the *Cisco ASA 5500 Series Release Notes* or the *Cisco PIX Security Appliance Release Notes*.



Note

The Cisco PIX 501 and PIX 506E security appliances are not supported.

This chapter includes the following sections:

- [New Features by Platform Release, page 2-1](#)
- [Firewall Functional Overview, page 2-12](#)
- [VPN Functional Overview, page 2-16](#)
- [Security Context Overview, page 2-16](#)

New Features by Platform Release

This section lists the new features available in each supported platform release. Because ASDM supports multiple platform releases, and this guide includes features for all releases, you should refer to these sections to determine if a feature is in your release. This section includes the following topics:

- [New Features in Version 8.1\(1\), page 2-2](#)
- [New Features in Version 8.0\(4\), page 2-2](#)
- [New Features in Version 8.0\(3\), page 2-5](#)
- [New Features in Version 8.0\(2\), page 2-6](#)

New Features in Version 8.1(1)

Table 2-1 lists the new features for Version 8.1(1).

Table 2-1 *New Features for ASA Version 8.1(1)*

Feature	Description
Introducing the Cisco ASA 5580	<ul style="list-style-type: none"> The Cisco ASA 5580 comes in two models: The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP performance is even greater. Many features in the system have been made multi-core capable to achieve this high throughput. In addition the system delivers greater than 60,000 TCP connections per second and supports up to 1 million connections. The ASA 5580-40 will deliver 10 Gigabits per second of TCP traffic and similar to ASA 5580-20 the UDP performance will be even greater. The ASA 5580-40 delivers greater than 120,000 TCP connections per second and up to 2 million connections in total.
NetFlow	The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information on this feature and the new CLI commands, see the Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide.

New Features in Version 8.0(4)

Table 2-2 lists the new features for Version 8.0(4).



Note

These features are not available in Version 8.1(1).

Table 2-2 *New Features for ASA Version 8.0(4)*

Feature	Description
Unified Communications Features	
Phone Proxy	<p>Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The ASA Phone Proxy has the following key features:</p> <ul style="list-style-type: none"> Secures remote IP phones by forcing the phones to encrypt signaling and media Performs certificate-based authentication with remote IP phones Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage (CUMA) servers Terminates SRTP and initiates RTP/SRTP to the called party

Table 2-2 **New Features for ASA Version 8.0(4) (continued)**

Feature	Description
TLS Proxy for Mobility Solution	<p>Secure connectivity (TLS proxy) between Cisco Unified Mobility Advantage (CUMA) clients and servers is supported.</p> <p>CUMA solutions include the Cisco Unified Mobile Communicator (CUMC), an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage (CUMA) server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise.</p> <p>The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, the proprietary protocol between CUMC and CUMA. The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between the CUMC and CUMA.</p>
TLS Proxy for Presence Federation	<p>Secure connectivity (TLS proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can securely connect their Cisco Unified Presence clients back to their enterprise networks, or share Presence information between Presence servers in different enterprises.</p> <p>The ASA delivers functionality to enable Presence for Internet and intra-enterprise communications. An SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence Server. The ASA enables SSL connectivity between server to server communication including third-party Presence servers communicating with Cisco Unified Presence servers. Enterprises share Presence information, and can use IM applications. The ASA inspects SIP messages between the servers.</p>
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE	<p>This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it isn't supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature.</p> <p>Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host.</p> <p>To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature does not support DAPs.</p>
Entrust Certificate Provisioning	<p>ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x) includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA. To use this feature, navigate to Configuration > Remote Access VPN > Certificate Management > Identity Certificates. Click Enroll ASA SSL VPN head-end with Entrust.</p>
Extended Time for User Reauthentication on IKE Rekey	<p>You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.</p>

Table 2-2 New Features for ASA Version 8.0(4) (continued)

Feature	Description
Persistent IPsec Tunneled Flows	With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a Hardware Client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels.
Show Active Directory Groups	The CLI command show ad-groups was added to list the active directory groups. This feature is useful for the configuration of DAP, which requires the administrator to know the names of the groups on a Microsoft LDAP Active Directory.
Smart Tunnel over Mac OS and Linux	Smart tunnels now support the Mac OS and Linux operating systems.
Firewall Features	
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the shape command. See also the crypto ipsec security-association replay command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing 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 become false alarms in the case of priority queueing. This new command avoids possible false alarms.</p>
TCP Normalization Enhancements	<p>You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.</p> <ul style="list-style-type: none"> • TCP invalid ACK check (the invalid-ack command) • TCP packet sequence past window check (the seq-past-window command) • TCP SYN-ACK with data check (the synack-data command) <p>You can also set the TCP out-of-order packet buffer timeout (the queue command timeout keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.</p> <p>The default action for packets that exceed MSS has changed from drop to allow (the exceed-mss command).</p> <p>The following non-configurable actions have changed from drop to clear for these packet types:</p> <ul style="list-style-type: none"> • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the threat-detection statistics tcp-intercept command, and view them using the show threat-detection statistics command.</p> <p>Note This feature is not currently supported in ASDM. You can enter this command using the Command Line Interface tool. See the <i>Cisco Security Appliance Command Reference</i> for more information.</p>

Table 2-2 **New Features for ASA Version 8.0(4) (continued)**

Feature	Description
Threat detection shun timeout	<p>You can now configure the shun timeout for threat detection using the threat-detection scanning-threat shun duration command.</p> <p>Note This feature is not currently supported in ASDM. You can enter this command using the Command Line Interface tool. See the <i>Cisco Security Appliance Command Reference</i> for more information.</p>
Timeout for SIP Provisional Media	<p>You can now configure the timeout for SIP provisional media using the timeout sip-provisional-media command.</p>
Platform Features	
Native VLAN support for the ASA 5505	<p>You can now include the native VLAN in an ASA 5505 trunk port using the switchport trunk native vlan command.</p> <p>Note This feature is not currently supported in ASDM. You can enter this command using the Command Line Interface tool. See the <i>Cisco Security Appliance Command Reference</i> for more information.</p>

New Features in Version 8.0(3)

Table 2-3 lists the new features for Version 8.0(3).

Table 2-3 **New Features for ASA Version 8.0(3)**

Feature	Description
AnyConnect RSA SoftID API Integration	<p>Provides support for AnyConnect VPN clients to communicate directly with RSA SoftID for obtaining user token codes. It also provides the ability to specify SoftID message support for a connection profile (tunnel group), and the ability to configure SDI messages on the security appliance that match SDI messages received through a RADIUS proxy. This feature ensures the prompts displayed to the remote client user are appropriate for the action required during authentication and the AnyConnect client responds successfully to authentication challenges.</p>

Table 2-3 *New Features for ASA Version 8.0(3) (continued)*

Feature	Description
IP Address Reuse Delay	Delays the reuse of an IP address after it has been returned to the IP address pool. Increasing the delay prevents problems the security appliance may experience when an IP address is returned to the pool and reassigned quickly.
WAAS and ASA Interoperability	<p>The [no] inspect waas command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The [no] inspect waas command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default.</p> <p>The keyword option waas is added to the show service-policy inspect command to display WAAS statistics.</p> <p>show service-policy inspect waas</p> <p>A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections.</p> <p>System Log Number and Format:</p> <p>%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.</p> <p>A new connection flag "W" is added in the WAAS connection. The show conn detail command is updated to reflect the new flag.</p>

New Features in Version 8.0(2)

Table 2-1 lists the new features for Version 8.0(2).



Note

There was no ASA 8.0(1) release.

Table 2-4 *New Features for ASA Version 8.0(2)*

ASA Feature Type	Feature	Description
General Features		
Routing	EIGRP routing	The security appliance supports EIGRP or EIGRP stub routing.

Table 2-4 ***New Features for ASA Version 8.0(2) (continued)***

ASA Feature Type	Feature	Description
High Availability	Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This works for both Active/Standby and Active/Active failover.
	CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature in failover configurations.
	Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configuration in failover pairs.
	Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
	Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs.
SSMs	Password reset	You can reset the password on the SSM hardware module.
VPN Features		
Authentication Enhancements	Combined certificate and username/password login	An administrator requires a username and password in addition to a certificate for login to SSL VPN connections.
	Internal domain username/password	Provides a password for access to internal resources for users who log in with credentials other than a domain username and password, for example, with a one-time password. This is a password in addition to the one a user enters when logging in.
	Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support available for authentication and authorization.
	Onscreen keyboard	The security appliance includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.
	SAML SSO verified with RSA Access Manager	The security appliance supports Security Assertion Markup Language (SAML) protocol for Single Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Identity Manager).
	NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-based clients.
Certificates	Local certificate authority	Provides a certificate authority on the security appliance for use with SSL VPN connections, both browser- and client-based.
	OCSP CRL	Provides OCSP revocation checking for SSL VPN.

Table 2-4 *New Features for ASA Version 8.0(2) (continued)*

ASA Feature Type	Feature	Description
Cisco Secure Desktop	Host Scan	<p>As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispymware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP).</p> <p>With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.</p> <p>Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.</p>
	Simplified prelogin assessment and periodic checks	<p>Cisco Secure Desktop now simplifies the configuration of prelogin and periodic checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. You can configure the security appliance to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.</p>
Access Policies	Dynamic access policies (DAP)	<p>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.</p> <p>Dynamic Access Policies (DAP) on the security appliance 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 security appliance grants access to a particular user for a particular session based on the policies you define. It 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.</p>
	Administrator differentiation	<p>Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS service-type attribute.</p>

Table 2-4 ***New Features for ASA Version 8.0(2) (continued)***

ASA Feature Type	Feature	Description
Platform Enhancements	VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPsec and SSL tunnel-based connections.
	VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 adaptive security appliances that have a Security Plus license.
	Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPsec operations and reducing the amount of debug output, you can better troubleshoot the security appliance with a large number of tunnels.
Browser-based SSL VPN Features	Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly organized and visually appealing.
	Customization	Supports administrator-defined customization of all user-visible content.
	Support for FTP	You can provide file access via FTP in addition to CIFS (Windows-based).
	Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications without requiring a pre-installed client application. Java applets let users access these applications from the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, RDP, and VNC.
	Smart tunnels	<p>A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with the security appliance as the pathway. Version 8.0(2) lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application and the SHA-1 hash of its checksum to check before granting it access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.</p> <p>The remote host originating the smart tunnel connection must be running Microsoft Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.</p>
	RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed information, which lets company news or other information display on a user screen.

Table 2-4 *New Features for ASA Version 8.0(2) (continued)*

ASA Feature Type	Feature	Description
Browser-based SSL VPN Features (continued)	Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a file server.
	Transformation enhancements	Adds support for several complex forms of web content over clientless connections, including Adobe flash and Java WebStart.
	IPv6	Allows access to IPv6 resources over a public IPv4 connection.
	Web folders	Lets browser-based SSL VPN users connecting from Windows operating systems browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.
	Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Microsoft Office applications available on the machine with the browser to view, change, and save documents shared on a server. Version 8.0(2) supports Windows Sharepoint Services 2.0 in Windows Server 2003.
HTTP Proxy	PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.
HTTPS Proxy	Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the security appliance can send to an external proxy server.
NAC	SSL VPN tunnel support	The security appliance provides NAC posture validation of endpoints that establish AnyConnect VPN client sessions.
	Support for audit services	You can configure the security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the security appliance for application to the traffic on the tunnel.

Table 2-4 New Features for ASA Version 8.0(2) (continued)

ASA Feature Type	Feature	Description
Firewall Features		
Application Inspection	Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.
	AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in WebVPN HTTP and HTTPS streams.
	TLS Proxy for SCCP and SIP	Enables inspection of encrypted traffic. Implementations include SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
	SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.
	Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.
Access Lists	Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.
	Ability to rename access list	Lets you rename an access list.
	Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.
Attack Prevention	Set connection limits for management traffic to the adaptive security appliance	For a Layer 3/4 management class map, you can specify the set connection command.
	Threat detection	You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.
NAT	Transparent firewall NAT support	You can configure NAT for a transparent firewall.
IPS	Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode adaptive security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

Table 2-4 **New Features for ASA Version 8.0(2) (continued)**

ASA Feature Type	Feature	Description
Logging	Secure logging	You can enable secure connections to the syslog server using SSL or TLS with TCP, and encrypted system log message content. Not supported on the PIX series adaptive security appliance.
IPv6	IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields.

Firewall Functional Overview

Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP server, you can place these resources on a separate network behind the firewall, called a *demilitarized zone* (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

When discussing networks connected to a firewall, the *outside* network is in front of the firewall, the *inside* network is protected and behind the firewall, and a *DMZ*, while behind the firewall, allows limited access to outside users. Because the security appliance lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

This section includes the following topics:

- [Security Policy Overview, page 2-12](#)
- [Firewall Mode Overview, page 2-15](#)
- [Stateful Inspection Overview, page 2-15](#)

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, the security appliance allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). You can apply actions to traffic to customize the security policy. This section includes the following topics:

- [Permitting or Denying Traffic with Access Lists, page 2-13](#)
- [Applying NAT, page 2-13](#)
- [Protecting from IP Fragments, page 2-13](#)
- [Using AAA for Through Traffic, page 2-13](#)
- [Applying HTTP, HTTPS, or FTP Filtering, page 2-13](#)
- [Applying Application Inspection, page 2-13](#)

- [Sending Traffic to the Advanced Inspection and Prevention Security Services Module, page 2-14](#)
- [Sending Traffic to the Content Security and Control Security Services Module, page 2-14](#)
- [Applying QoS Policies, page 2-14](#)
- [Applying Connection Limits and TCP Normalization, page 2-14](#)

Permitting or Denying Traffic with Access Lists

You can apply an access list to limit traffic from inside to outside, or allow traffic from outside to inside. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.

Applying NAT

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Protecting from IP Fragments

The security appliance provides IP fragment protection. This feature performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the security appliance. Fragments that fail the security check are dropped and logged. Virtual reassembly cannot be disabled.

Using AAA for Through Traffic

You can require authentication and/or authorization for certain types of traffic, for example, for HTTP. The security appliance also sends accounting information to a RADIUS or TACACS+ server.

Applying HTTP, HTTPS, or FTP Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet. We recommend that you use the security appliance in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise
- Secure Computing SmartFilter

Applying Application Inspection

Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the security appliance to do a deep packet inspection.

Sending Traffic to the Advanced Inspection and Prevention Security Services Module

If your model supports the AIP SSM for intrusion prevention, then you can send traffic to the AIP SSM for inspection. The AIP SSM is an intrusion prevention services module that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. Other legitimate connections continue to operate independently without interruption. For more information, see *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

Sending Traffic to the Content Security and Control Security Services Module

If your model supports it, the CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure the adaptive security appliance to send to it.

Applying QoS Policies

Some network traffic, such as voice and streaming video, cannot tolerate long latency times. QoS is a network feature that lets you give priority to these types of traffic. QoS refers to the capability of a network to provide better service to selected network traffic.

Applying Connection Limits and TCP Normalization

You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The security appliance uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

TCP normalization is a feature consisting of advanced TCP connection settings designed to drop packets that do not appear normal.

Enabling Threat Detection

You can configure scanning threat detection and basic threat detection, and also how to use statistics to analyze threats.

Basic threat detection detects activity that might be related to an attack, such as a DoS attack, and automatically sends a system log message.

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the security appliance scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

You can configure the security appliance to send system log messages about an attacker or you can automatically shun the host.

Firewall Mode Overview

The security appliance runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the security appliance is considered to be a router hop in the network.

In transparent mode, the security appliance acts like a “bump in the wire,” or a “stealth firewall,” and is not considered a router hop. The security appliance connects to the same network on its inside and outside interfaces.

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams using an EtherType access list.

Stateful Inspection Overview

All traffic that goes through the security appliance is inspected using the Adaptive Security Algorithm and either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the security appliance, however, takes into consideration the state of a packet:

- Is this a new connection?

If it is a new connection, the security appliance has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the “session management path,” and depending on the type of traffic, it might also pass through the “control plane path.”

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the “fast path”

**Note**

The session management path and the fast path make up the “accelerated security path.”

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels: a data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.

- Is this an established connection?

If the connection is already established, the security appliance does not need to re-check packets; most matching packets can go through the fast path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification

- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

For UDP or other connectionless protocols, the security appliance creates connection state information so that it can also use the fast path.

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

VPN Functional Overview

A VPN is a secure connection across a TCP/IP network (such as the Internet) that appears as a private connection. This secure connection is called a tunnel. The security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance 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 security appliance invokes various standard protocols to accomplish these functions.

The security appliance performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

The security appliance invokes various standard protocols to accomplish these functions.

Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration,

which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs into the admin context, then that user has system administrator rights and can access the system and all other contexts.

**Note**

You can run all your contexts in routed mode or transparent mode; you cannot run some contexts in one mode and others in another.

Multiple context mode supports static routing only.



CHAPTER 3

Defining Preferences and Using Configuration, Diagnostic, and File Management Tools

This chapter describes the preferences and tools available for configuration, problem diagnosis, and file management, and includes the following sections:

- [Preferences, page 3-1](#)
- [Configuration Tools, page 3-3](#)
- [Diagnostic Tools, page 3-7](#)
- [File Management Tools, page 3-18](#)

Preferences

This feature lets you change the behavior of some ASDM functions between sessions.

To change various settings in ASDM, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
- The Preferences dialog box appears, with three tabs: General, Rules Table, and Syslog Colors.
- Step 2** Click one of these tabs to define your settings: the **General** tab to specify general preferences; the **Rules Tables** tab to specify preferences for the Rules table; and the **Syslog Colors** tab to specify the background, foreground, and text colors for syslog messages displayed in the Home pane.
- Step 3** On the General tab, specify the following:
- a. Check the **Preview commands before sending them to the device** check box to view CLI commands generated by ASDM.
 - b. Check the **Enable cumulative (batch) CLI delivery** check box to send multiple commands in a single group to the adaptive security appliance.
 - c. Check the **Warn that configuration in ASDM is out of sync with the configuration in ASA** check box to be notified when the startup configuration and the running configuration are no longer in sync with each other.
 - d. Check the **Confirm before exiting ASDM** check box to display a prompt when you try to close ASDM to confirm that you want to exit. This option is checked by default.
 - e. Check the **Show configuration restriction message to read-only user** check box to display the following message to a read-only user at startup. This option is checked by default.

"You are not allowed to modify the ASA configuration, because you do not have sufficient privileges."

- f. Check the **Enable screen reader support (requires ASDM restart)** check box to enable screen readers to work. You must restart ASDM to enable this option.
- g. To allow the Packet Capture Wizard to display captured packets, enter the name of the network sniffer application or click **Browse** to find it.

Step 4 On the Rules Tables tab, specify the following:

- a. Display settings let you change the way rules are displayed in the Rules table.
 - Check the **Auto-expand network and service object groups with specified prefix** check box to display the network and service object groups automatically expanded based on the Auto-Expand Prefix setting.
 - In the Auto-Expand Prefix field, specify the prefix of the network and service object groups to expand automatically when displayed.
 - Check the **Show members of network and service object groups** check box to display members of network and service object groups and the group name in the Rules table. If the check box is not checked, only the group name is displayed.
 - In the Limit Members To field, enter the number of network and service object groups to display. When the object group members are displayed, then only the first *n* members are displayed.
 - Check the **Show all actions for service policy rules** check box to display all actions in the Rules table. When unchecked, a summary is displayed.
- b. Deployment settings let you configure the behavior of the security appliance when deploying changes to the Rules table.
 - Check the **Issue "clear xlate" command when deploying access lists** check box to clear the NAT table when deploying new access lists. This setting ensures the access lists that are configured on the security appliance are applied to all translated addresses.
- c. Access Rule Hit Count Settings let you configure the frequency for which the hit counts are updated in the Access Rules table. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
 - Check the **Update access rule hit counts automatically** check box to have the hit counts automatically updated in the Access Rules table.
 - In the Update Frequency field, specify the frequency in seconds that the hit count column is updated in the Access Rules table. Valid values are 10 - 86400 seconds.

Step 5 On the Syslog Colors tab, specify the following:

- To change the background text or foreground text color for messages at each severity level, click the corresponding column. The Pick a Color dialog box appears. Click one of the following tabs:
 - On the Swatches tab, choose a color from the palette, and click **OK**.
 - On the HSB tab, specify the H, S, and B settings, and click **OK**.
 - On the RGB tab, specify the Red, Green, and Blue settings, and click **OK**.

Severity is a non-editable column that lists each severity level by name and number.

**Note**

Each time a preference is checked or unchecked, the change is saved to the .conf file and becomes available for all the other ASDM sessions running on the workstation at the time. You must restart ASDM for all changes to take effect.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Configuration Tools

This section includes the following topics:

- [Reset Device to the Factory Default Configuration, page 3-3](#)
- [Save Running Configuration to TFTP Server, page 3-4](#)
- [Save Internal Log Buffer to Flash, page 3-5](#)
- [Command Line Interface, page 3-5](#)
- [Show Commands Ignored by ASDM on Device, page 3-6](#)

Reset Device to the Factory Default Configuration

The default configuration provides the minimum commands required to connect to the adaptive security appliance using ASDM.

**Note**

This feature is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces. In addition, this feature is available only in single context mode; a security appliance with a cleared configuration does not have any defined contexts to configure automatically using this feature.

To reset the adaptive security appliance to the factory default configuration, perform the following steps:

- Step 1** In the main ASDM application window, choose **File > Reset Device to the Factory Default Configuration**.

The Reset Device to the Default Configuration dialog box appears.

- Step 2** Enter the Management IP address of the management interface, instead of using the default address, 192.168.1.1. For an adaptive security appliance with a dedicated management interface, the interface is called “Management0/0.” For other adaptive security appliances, the configured interface is Ethernet 1 and called “inside.”

Step 3 Choose the Management (or Inside) Subnet Mask from the drop-down list.

Step 4 To save this configuration to internal flash memory, choose **File > Save Running Configuration to Flash**.

Selecting this option saves the running configuration to the default location for the startup configuration, even if you have previously configured a different location for the [System Time](#). When the configuration was cleared, this path was also cleared. The next time you reload the adaptive security appliance after restoring the factory configuration, the device boots from the first image in internal flash memory. If an image in internal flash memory does not exist, the adaptive security appliance does not boot.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Save Running Configuration to TFTP Server

This feature stores a copy of the current running configuration file on a TFTP server.

To save the running configuration to a TFTP server, perform the following steps:

Step 1 In the main ASDM application window, choose **File > Save Running Configuration to TFTP Server**.

The Save Running Configuration to TFTP Server dialog box appears.

Step 2 Enter the TFTP server IP address and file path on the TFTP server in which the configuration file will be saved, and then click **Save Configuration**.



Note To configure default TFTP settings, choose **Configuration > Device Management > Management Access > File Access > TFTP Client**. After you have configured this setting, the TFTP server IP address and file path on the TFTP server appear automatically in this dialog box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Save Internal Log Buffer to Flash

This feature lets you save the internal log buffer to flash memory.

To save the internal log buffer to flash memory, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **File > Save Internal Log Buffer to Flash**.
The Enter Log File Name dialog box appears.
 - Step 2** Choose the first option to save the log buffer with the default filename, LOG-YYYY-MM-DD-hhmmss.txt.
 - Step 3** Choose the second option to specify a filename for the log buffer.
 - Step 4** Enter the filename for the log buffer, and then click **OK**.
-

Command Line Interface

This feature provides a text-based tool for sending commands to the adaptive security appliance and viewing the results.

The commands you can enter with the CLI tool depend on your user privileges. See the section, [About Authorization](#) for more information. Review your privilege level in the status bar at the bottom of the main ASDM application window to ensure that you have the required privileges to execute privileged-level CLI commands.



Note

Commands entered via the ASDM CLI tool might function differently from those entered through a terminal connection to the adaptive security appliance.

To use the CLI tool, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Command Line Interface**.
The Command Line Interface dialog box appears.
 - Step 2** Choose the type of command (single line or multiple line) that you want, and then choose the command from the drop-down list, or type it in the field provided.
 - Step 3** Click **Send** to execute the command.
 - Step 4** To enter a new command, click **Clear Response**, and then choose (or type) another command to execute.
 - Step 5** Check the **Enable context-sensitive help (?)** check box to provide context-sensitive help for this feature. Uncheck this check box to disable the context-sensitive help.
 - Step 6** After you have closed the Command Line Interface dialog box, if you changed the configuration, click **Refresh** to view the changes in ASDM.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Command Errors

If an error occurs because you entered an incorrect command, the incorrect command is skipped and the remaining commands are processed. A message displays in the Response area to inform you whether any error occurred, as well as other related information.



Note

ASDM supports almost all CLI commands. See the *Cisco Security Appliance Command Reference* for a list of commands.

Interactive Commands

Interactive commands are not supported in the CLI tool. To use these commands in ASDM, use the **noconfirm** keyword if available, as shown in the following command:

```
crypto key generate rsa modulus 1024 noconfirm
```

Avoiding Conflicts with Other Administrators

Multiple administrative users can update the running configuration of the adaptive security appliance. Before using the ASDM CLI tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the adaptive security appliance at the same time, the most recent changes take effect.

To view other administrative sessions that are currently active on the same adaptive security appliance, choose **Monitoring > Properties > Device Access**.

Show Commands Ignored by ASDM on Device

This feature lets you show the list of commands that ASDM does not support. Typically, ASDM ignores them. ASDM does not change or remove these commands from your running configuration. See [Unsupported Commands](#) for more information.

To display the list of unsupported commands for ASDM, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Show Commands Ignored by ASDM on Device**.
 - Step 2** Click **OK** when you are done.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Diagnostic Tools

ASDM provides a set of diagnostic tools to help you in troubleshooting problems. This section includes the following topics:

- [Packet Tracer, page 3-7](#)
- [Ping, page 3-8](#)
- [Traceroute, page 3-11](#)
- [Administrator's Alert to Clientless SSL VPN Users, page 3-12](#)
- [ASDM Java Console, page 3-12](#)
- [Packet Capture Wizard, page 3-13](#)

Packet Tracer

The packet tracer tool provides packet tracing for packet sniffing and network fault isolation, as well as detailed information about the packets and how they are processed by the adaptive security appliance. If a configuration command did not cause the packet to drop, the packet tracer tool will provide information about the cause in an easily readable manner. For example, if a packet was dropped because of an invalid header validation, the following message is displayed:

```
"packet dropped due to bad ip header (reason)."
```

In addition to capturing packets, you can trace the lifespan of a packet through the adaptive security appliance to see whether the packet is behaving as expected. The packet tracer tool lets you do the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet, along with the CLI lines that caused the rule addition.
- Show a time line of packet changes in a data path.
- Trace packets in the data path.

To open the packet tracer, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Packet Tracer**.
The Cisco ASDM Packet Tracer dialog box appears.
 - Step 2** Choose the source interface for the packet trace from the drop-down list.
 - Step 3** Specify the protocol type for the packet trace. Available protocol types are ICMP, IP, TCP, and UDP.
 - Step 4** Enter the source address for the packet trace in the Source IP Address field.

- Step 5** Choose the source port for the packet trace from the drop-down list.
- Step 6** Enter the destination IP address for the packet trace in the Destination IP Address field.
- Step 7** Choose the destination port for the packet trace from the drop-down list.
- Step 8** Click **Start** to trace the packet.

The Information Display Area shows detailed messages about the packet trace.



Note To display a graphical representation of the packet trace, check the **Show animation** check box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Ping

The Ping tool is useful for verifying the configuration and operation of the adaptive security appliance and surrounding communications links, as well as for testing other network devices.

A ping is sent to an IP address and it returns a reply. This process enables network devices to discover, identify, and test each other.

The Ping tool uses ICMP (as described in RFC-777 and RFC-792) to define an echo request and reply transaction between two network devices. The echo request packet is sent to the IP address of a network device. The receiving device reverses the source and destination address and sends the packet back as the echo reply.

To use the Ping tool, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Ping**.
The Ping dialog box appears.
- Step 2** Enter the destination IP address for the ICMP echo request packets in the IP Address field.



Note If a hostname has been assigned in the Configuration > Firewall > Objects > IP Names pane, you can use the hostname in place of the IP address.

- Step 3** (Optional) Choose the security appliance interface that transmits the echo request packets from the drop-down list. If it is not specified, the security appliance checks the routing table to find the destination address and uses the required interface.
- Step 4** Click **Ping** to send an ICMP echo request packet from the specified or default interface to the specified IP address and start the response timer.

The response appears in the Ping Output area. Three attempts are made to ping the IP address, and results display the following fields:

- The IP address of the device pinged or a device name, if available. The name of the device, if assigned Hosts/Networks, may be displayed, even if **NO response** is the result.
- When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This timer is useful for testing the relative response times of different routes or activity levels.
- Example Ping output:

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
If the ping fails, the output is as follows:
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
????
Success rate is 0 percent (0/5)
```

Step 5 To enter a new IP address, click **Clear Screen** to remove the previous response from the Ping output area.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Using the Ping Tool

Administrators can use the ASDM Ping interactive diagnostic tool in these ways:

- Loopback testing of two interfaces—A ping may be initiated from one interface to another on the same security appliance, as an external loopback test to verify basic “up” status and operation of each interface.
- Pinging to a security appliance—The Ping tool can ping an interface on another security appliance to verify that it is up and responding.
- Pinging through a security appliance—Ping packets originating from the Ping tool may pass through an intermediate security appliance on their way to a device. The echo packets will also pass through two of its interfaces as they return. This procedure can be used to perform a basic test of the interfaces, operation, and response time of the intermediate unit.
- Pinging to test questionable operation of a network device—A ping may be initiated from an adaptive security appliance interface to a network device that is suspected to be functioning incorrectly. If the interface is configured correctly and an echo is not received, there may be problems with the device.
- Pinging to test intermediate communications—A ping may be initiated from an adaptive security appliance interface to a network device that is known to be functioning correctly and returning echo requests. If the echo is received, the correct operation of any intermediate devices and physical connectivity is confirmed.

Troubleshooting the Ping Tool

When pings fail to receive an echo, it may be the result of a configuration or operational error in an adaptive security appliance, and not necessarily because of no response from the IP address being pinged. Before using the Ping tool to ping from, to, or through an adaptive security appliance interface, perform the following basic checks:

- Verify that interfaces are configured by choosing **Configuration > Device Setup > Interfaces**.
- Verify that devices in the intermediate communications path, such as switches or routers, are correctly delivering other types of network traffic.
- Make sure that traffic of other types from “known good” sources is being passed by choosing **Monitoring > Interfaces > Interface Graphs**.

Pinging from a Security Appliance Interface

For basic testing of an interface, you can initiate a ping from an adaptive security appliance interface to a network device that you know is functioning correctly and returning replies via the intermediate communications path. For basic testing, make sure you do the following:

- Verify receipt of the ping from the adaptive security appliance interface by the “known good” device. If the ping is not received, a problem with the transmitting hardware or interface configuration may exist.
- If the adaptive security appliance interface is configured correctly and it does not receive an echo reply from the “known good” device, problems with the interface hardware receiving function may exist. If a different interface with “known good” receiving capability can receive an echo after pinging the same “known good” device, the hardware receiving problem of the first interface is confirmed.

Pinging to a Security Appliance Interface

When you try to ping to an adaptive security appliance interface, verify that the pinging response (ICMP echo reply) is enabled for that interface by choosing **Tools > Ping**. When pinging is disabled, the adaptive security appliance cannot be detected by other devices or software applications, and will not respond to the ASDM Ping tool.

Pinging Through the Security Appliance

To verify that other types of network traffic from “known good” sources is being passed through the adaptive security appliance, choose **Monitoring > Interfaces > Interface Graphs** or an SNMP management station.

To enable internal hosts to ping external hosts, configure ICMP access correctly for both the inside and outside interfaces by choosing **Configuration > Firewall > Objects > IP Names**.

Traceroute

The Traceroute tool helps you to determine the route that packets will take to their destination. The tool prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following table lists the output symbols printed by this tool:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
<i>nn msec</i>	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

To use the Traceroute tool, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Traceroute**.
The Traceroute dialog box appears.
 - Step 2** Enter the name of the host to which the route is traced. If the hostname is specified, define it by choosing **Configuration > Firewall > Objects > IP Names**, or configure a DNS server to enable this tool to resolve the hostname to an IP address.
 - Step 3** Enter the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
 - Step 4** Type the destination port used by the UDP probe messages. The default is 33434.
 - Step 5** Enter the number of probes to be sent at each TTL level. The default is three.
 - Step 6** Specify the minimum and maximum TTL values for the first probes. The minimum default is one, but it can be set to a higher value to suppress the display of known hops. The maximum default is 30. The traceroute terminates when the packet reaches the destination or when the maximum value is reached.
 - Step 7** Check the **Specify source interface or IP address** check box. Choose the source interface or IP address for the packet trace from the drop-down list. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the adaptive security appliance.
 - Step 8** Check the **Reverse Resolve** check box to have the output display the names of hops encountered if name resolution is configured. Leave this check box unchecked to have the output display IP addresses.
 - Step 9** Check the **Use ICMP** check box to specify the use of ICMP probe packets instead of UDP probe packets.
 - Step 10** Click **Trace Route** to start the traceroute.
The Traceroute Output area displays detailed messages about the traceroute results.
 - Step 11** Click **Clear Output** to start a new traceroute.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Administrator's Alert to Clientless SSL VPN Users

This feature lets you send an alert message to clientless SSL VPN users (for example, about connection status).

To send an alert message, perform the following steps:

Step 1 In the main ASDM application window, choose **Tools > Administrator's Alert Message to Clientless SSL VPN Users**.

The Administrator's Alert Message to Clientless SSL VPN Users dialog box appears.

Step 2 Enter the new or edited alert content that you want to send, and then click **Post Alert**.

Step 3 To remove current alert content and enter new alert content, click **Cancel Alert**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

ASDM Java Console

You can use the ASDM Java console to view and copy logged entries in a text format, which can help you troubleshoot ASDM errors. To access this tool, in the main ASDM application window, choose **Tools > ASDM Java Console**.

To show the virtual machine memory statistics, enter **m** in the console.

To perform garbage collection, enter **g** in the console.

To monitor memory usage, open the Windows Task Manager and double-click the **asdm_launcher.exe** file.

**Note**

The maximum memory allocation allowed is 256 MB.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Packet Capture Wizard

You can use the Packet Capture Wizard to configure and run captures for troubleshooting errors. The captures can use access lists to limit the type of traffic captured, the source and destination addresses and ports, and one or more interfaces. The wizard runs one capture on each of the ingress and egress interfaces. You can save the captures on your PC to examine them in a packet analyzer.



Note

This tool does not support clientless SSL VPN capture.

To configure and run captures, perform the following steps:

- Step 1** In the main ASDM application window, choose **Wizards > Packet Capture Wizard**.
The Overview of Packet Capture screen appears, with a list of the tasks that the wizard will guide you through to complete.
- Step 2** Click **Next** to display the Ingress Traffic Selector screen.
- Step 3** Choose the ingress interface (inside or outside) from the drop-down list.
- Step 4** Enter the source host IP address and choose the network IP address from the drop-down list.
- Step 5** Choose the protocol from the drop-down list.
- Step 6** Depending on the selected protocol, you also need to define both the source port services and destination port services. Choose one of the following options:
 - All Services
 - Service group, which you choose from the drop-down list
 - Service, which you choose according to a set of predefined parameters
- Step 7** Click **Next** to display the Egress Traffic Selector screen.
- Step 8** Choose the egress interface from the drop-down list.
- Step 9** Enter the source host IP address and choose the network IP address from the drop-down list.



Note

The source port services and destination port services are read-only based on the choices you made in the Ingress Traffic Selector screen.

- Step 10** Click **Next** to display the Buffers screen. The buffer size is the maximum amount of memory that the capture can use to store packets. The packet size is the longest packet that the capture can hold. We recommend that you use the longest packet size to capture as much information as possible.

- Step 11** Enter the packet size. The valid size ranges from 14 - 1522 bytes.
- Step 12** Enter the buffer size. The valid size ranges from 1534 - 33554432 bytes.
- Step 13** Check the **Use circular buffer** check box to store captured packets.



Note When you choose this setting, if all the buffer storage is used, the capture will start overwriting the oldest packets.

- Step 14** Click **Next** to display the Summary screen, which shows the traffic selectors and buffer parameters that you have entered.
- Step 15** Click **Next** to display the Run Capture screen, and then click **Start** to begin capturing packets. Click **Stop** to end the capture.
- Step 16** Click **Get Capture Buffer** to determine how much buffer space you have remaining. Click **Clear Buffer on Device** to remove the current content and allow room in the buffer to capture more packets.
- Step 17** Click **Save captures** to display the Save Capture dialog box. Select the format in which you want to include the captures: **ASCII** or **PCAP**. You have the option of saving either the ingress capture, the egress capture, or both.
- Step 18** To save the ingress packet capture, click **Save Ingress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.
- Step 19** To save the egress packet capture, click **Save Egress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.
- Step 20** Click **Close**, and then click **Finish** to exit the wizard.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Field Information for the Packet Capture Wizard

This section includes the following topics:

- [Ingress Traffic Selector, page 3-15](#)
- [Egress Traffic Selector, page 3-15](#)
- [Buffers, page 3-16](#)
- [Summary, page 3-16](#)
- [Run Captures, page 3-17](#)
- [Save Captures, page 3-17](#)

Ingress Traffic Selector

The Ingress Traffic Selector dialog box lets you configure the ingress interface, source and destination hosts/networks, and the protocol for packet capture.

Fields

- Ingress Interface—Specifies the ingress interface name.
- Source Host/Network—Specifies the ingress source host and network.
- Destination Host/Network—Specifies the ingress destination host and network.
- Protocol—Specifies the protocol type to capture (ah, eigrp, esp, gre, icmp, icmp6, igmp, igmp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp, or udp).
 - ICMP type—Specifies the ICMP type for ICMP protocol only (all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute, or unreachable).
 - Source/Destination Port Services—Specifies source and destination port services for TCP and UDP protocols only.

All Services—Specifies all services.

Service Group—Specifies a service group.

Service—Specifies a service (aol, bgp, chargen, cifs, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, pcanywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, or whois).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Egress Traffic Selector

The Egress Traffic Selector dialog box lets you configure the egress interface, source and destination hosts/networks, and source and destination port services for packet capture.

Fields

- Egress Interface—Specifies the egress interface name.
- Source Host/Network—Specifies the egress source host and network.
- Destination Host/Network—Specifies the egress destination host and network.
- Protocol—Specifies the protocol type selected during the ingress configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Buffers

The Buffers dialog box lets you configure the packet size, buffer size, and whether to use the circular buffer for packet capture.

Fields

- **Packet Size**—Specifies longest packet that the capture can hold. Use the longest size available to capture as much information as possible.
- **Buffer Size**—Specifies the maximum amount of memory that the capture can use to store packets.
- **Use circular buffer**—Specifies whether to use the circular buffer to store packets. When the circular buffer has used all of the buffer storage, the capture will write over the oldest packets first.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Summary

The Summary dialog box shows the traffic selectors and the buffer parameters for the packet capture.

Fields

- **Traffic Selectors**—Shows the capture and access list configuration specified in the previous steps.
- **Buffer Parameters**—Shows the buffer parameters specified in the previous step.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Run Captures

The Run Captures dialog box lets you start and stop the capture session. You can also view the capture buffer, launch a network analyzer application, save the packet captures, and clear the buffer.

Fields

- **Start**—Starts the packet capture session on selected interfaces.
- **Stop**—Stops the packet capture session on selected interfaces.
- **Get Capture Buffer**—Specifies to show a snapshot of the captured packets on the interface.
- **Ingress**—Shows the capture buffer on the ingress interface.
 - **Launch Network Sniffer Application**—Launches the packet analysis application specified in Tools > Preferences for analyzing the ingress capture.
- **Egress**—Shows the capture buffer on the egress interface.
 - **Launch Network Sniffer Application**—Launches the packet analysis application specified in Tools > Preferences for analyzing the egress capture.
- **Save Captures**—Lets you save the ingress and egress captures in either ASCII or PCAP format.
- **Clear Buffer on Device**—Clears the buffer on the device.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Save Captures

The Save Captures dialog box lets you save the ingress and egress packet captures to ASCII or PCAP file format for further packet analysis.

Fields

- **ASCII**—Specifies to save the capture buffer in ASCII format.
- **PCAP**—Specifies to save the capture buffer in PCAP format.
- **Save ingress capture**—Lets you specify a file to save the ingress packet capture.
- **Save egress capture**—Lets you specify a file to save the egress packet capture.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

File Management Tools

ASDM provides a set of file management tools to help you perform basic file management tasks. This section includes the following topics:

- [File Management, page 3-18](#)
- [Manage Mount Points, page 3-19](#)
- [Add/Edit a CIFS/FTP Mount Point, page 3-19](#)
- [Upgrade Software from Local Computer, page 3-20](#)
- [File Transfer, page 3-21](#)
- [Upgrade Software from Cisco.com Wizard, page 3-23](#)
- [ASDM Assistant, page 3-24](#)
- [System Reload, page 3-25](#)
- [Backup and Restore, page 3-26](#)

File Management

The File Management tool lets you view, move, copy, and delete files stored in flash memory, transfer files, and to manage files on remote storage devices (mount points).



Note

In multiple context mode, this tool is only available in the system security context.

To use the file management tools, perform the following steps:

Step 1 In the main ASDM application window, choose **Tools > File Management**.

The File Management dialog box appears.

- The Folders pane displays the available folders on disk.
- Flash Space shows the total amount of flash memory and how much memory is available.
- The Files area displays the following information about files in the selected folder:
 - Path
 - Filename
 - Size (bytes)
 - Time Modified

- Status, which indicates whether a selected file is designated as a boot configuration file, boot image file, ASDM image file, SVC image file, CSD image file, or APCF image file.

- Step 2** Click **View** to display the selected file in your browser.
- Step 3** Click **Cut** to cut the selected file for pasting to another directory.
- Step 4** Click **Copy** to copy the selected file for pasting to another directory.
- Step 5** Click **Paste** to paste the copied file to the selected destination.
- Step 6** Click **Delete** to remove the selected file from flash memory.
- Step 7** Click **Rename** to rename a file.
- Step 8** Click **New Directory** to create a new directory for storing files.
- Step 9** Click **File Transfer** to open the File Transfer dialog box. See [File Transfer, page 3-21](#) for more information.
- Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See [Manage Mount Points, page 3-19](#) for more information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Manage Mount Points

This feature lets you configure remote storage (mount points) for network file systems using a CIFS or FTP connection. The dialog box lists the mount-point name, connection type, server name or IP address, and the enabled setting (yes or no). You can add, edit, or delete mount points. See [Add/Edit a CIFS/FTP Mount Point, page 3-19](#) for more information.



Note

On a PIX 535 security appliance in single, routed mode, the Manage Mount Point feature is not available.

Add/Edit a CIFS/FTP Mount Point

To add a CIFS mount point, perform the following steps:

- Step 1** Click **Add**, and then choose **CIFS Mount Point**.
The Add CIFS Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
- Step 2** Enter the mount-point name, server name or IP address, and share name in the applicable fields.

- Step 3** In the Authentication section, enter the NT domain, username and password, and then confirm the password.
- Step 4** Click **OK**.

To add an FTP mount point, perform the following steps:

- Step 1** Click **Add**, and then choose **FTP Mount Point**.
The Add FTP Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
- Step 2** Enter the mount-point name and the server name or IP address in the applicable fields.
- Step 3** In the FTP Mount Options area, click the **Active Mode** or **Passive Mode** option.
- Step 4** Enter the path to mount the remote storage.
- Step 5** In the Authentication area, enter the NT domain, username and password, and then confirm the password.
- Step 6** Click **OK**.

To edit a CIFS mount point, perform the following steps:

- Step 1** Choose the CIFS mount-point you want to modify, and click **Edit**.
The Edit CIFS Mount Point dialog box appears.



Note You cannot change the CIFS mount-point name.

- Step 2** Make the changes to the remaining settings, and click **OK** when you are done.

To edit an FTP mount point, perform the following steps:

- Step 1** Choose the FTP mount-point you want to modify, and click **Edit**.
The Edit FTP Mount Point dialog box appears.



Note You cannot change the FTP mount-point name.

- Step 2** Make the changes to the remaining settings, and click **OK** when you are done.

Upgrade Software from Local Computer

The Upgrade Software from Local Computer tool lets you upload an image file from your PC to the flash file system to upgrade the adaptive security appliance.

To upgrade software from your PC, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.
 - Step 2** Choose the image file to upload from the drop-down list.
 - Step 3** Enter the local path to the file on your PC or click **Browse Local Files** to find the file on your PC.
 - Step 4** Enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
 - Step 5** Click **Image to Upload**. The uploading process might take a few minutes; make sure you wait until it is finished.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

File Transfer

The File Transfer tool lets you transfer files from either a local or remote location. You can transfer a local file on your computer or a flash file system to and from the security appliance. You can transfer a remote file to and from the security appliance using HTTP, HTTPS, TFTP, FTP, or SMB.

To transfer files between your local computer and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**. The File Management dialog box appears.
 - Step 2** Click the down arrow next to **File Transfer**, and then click **Between Local PC and Flash**. The File Transfer dialog box appears.
 - Step 3** Select and *drag* the file(s) from either your local computer or the flash file system that you want to upload or download to the desired location. Alternatively, select the file(s) from either your local computer or the flash file system that you want to upload or download, and click the right arrow or left arrow to transfer the file(s) to the desired location.
 - Step 4** Click **Close** when you are done.
-

To transfer files between a remote server and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**. The File Management dialog box appears.

- Step 2** Click the down arrow next to **File Transfer**, and then click **Between Remote Server and Flash**.
The File Transfer dialog box appears.
- Step 3** To transfer a file from a remote server, click the **Remote server** option.
- Step 4** Define the source file to be transferred.
- a. Choose the path to the location of the file, including the IP address of the server.
 - b. Enter the port number or type (if FTP) of the remote server. Valid FTP types are the following:
 - ap—ASCII files in passive mode
 - an—ASCII files in non-passive mode
 - ip—Binary image files in passive mode
 - in—Binary image files in non-passive mode
- Step 5** To transfer the file from the flash file system, click the **Flash file system** option.
- Step 6** Enter the path to the location of the file or click **Browse Flash** to find the file location.
- Step 7** In addition, you can copy a file from your startup configuration, running configuration, or an SMB file system through the CLI. For instructions about using the **copy** command, see the *Cisco Security Appliance Command Line Configuration Guide*.
- Step 8** Define the destination of the file to be transferred.
- a. To transfer the file to the flash file system, choose the **Flash file system** option.
 - b. Enter the path to the location of the file or click **Browse Flash** to find the file location.
- Step 9** To transfer a file to a remote server, choose the **Remote server** option.
- a. Enter the path to the location of the file.
 - b. For FTP transfers, enter the type. Valid types are the following:
 - ap—ASCII files in passive mode
 - an—ASCII files in non-passive mode
 - ip—Binary image files in passive mode
 - in—Binary image files in non-passive mode
- Step 10** Click **Transfer** to start the file transfer.
The Enter Username and Password dialog box appears.
- Step 11** Enter the username, password, and domain (if required) for the remote server.
- Step 12** Click **OK** to continue the file transfer.
The file transfer process might take a few minutes; make sure that you wait until it is finished.
- Step 13** Click **Close** when the file transfer is finished.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Upgrade Software from Cisco.com Wizard

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and adaptive security appliance to more current versions.



Note

This feature is not available in the user or admin context mode in a single security context.

In this wizard, you can do the following:

- Download the list of available releases from Cisco.com.
- Select an ASDM image file or ASA image file for upgrade.
- Upgrade the images you have selected.
- Reload the firewall if you have upgraded the ASA image (optional).



Note

You must upgrade incrementally from one version to the next (for example, from Version 5.1 to 5.2, from Version 5.2 to 6.0(2), and so on). You cannot upgrade from Version 5.1 to 6.0(2).

To upgrade software from Cisco.com, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Cisco.com**.
The Upgrade Software from Cisco.com Wizard appears. The Overview screen describes the steps in the image upgrade process.
- Step 2** Click **Next** to continue.
The Authentication screen appears.
- Step 3** Enter your assigned Cisco.com user name and the Cisco.com password, and then click **Next**.
The Image Selection screen appears.
- Step 4** Choose one or both of the two options listed.
 - Check the **Upgrade the ASA version** check box to specify the most current adaptive security appliance image to which you want to upgrade.
 - Check the **Upgrade the ASDM version** check box to specify the most current ASDM version to which you want to upgrade.



Note

If the ASA version list or the ASDM version list is empty, a statement appears informing you that no new ASA or ASDM images are available. If you see this statement, you can exit the wizard.

Step 5 Click **Next** to continue.

The Selected Images screen appears.

Step 6 Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.

The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.

The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the adaptive security appliance.

If you upgraded the adaptive security appliance version and the upgrade succeeded, an option to save the configuration and reload the adaptive security appliance appears.

Step 7 Click **Yes**.

For the upgrade versions to take effect, you must save the configuration, reload the adaptive security appliance, and restart ASDM.



Note You do not need to restart the wizard after you have completed one incremental upgrade. You can return to [Step 3](#) of the wizard to upgrade to the next higher version, if any.

Step 8 Click **Finish** to exit the wizard when the upgrade is finished.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

ASDM Assistant

The ASDM Assistant tool lets you search and view useful ASDM procedural help about certain tasks.

To access information, choose **View > ASDM Assistant > How Do I?** or enter a search request from the Look For field in the menu bar. From the Find drop-down list, choose **How Do I?** to begin the search.



Note This feature is not available on the PIX security appliance.

To view the ASDM Assistant, perform the following steps:

Step 1 In the main ASDM application window, choose **View > ASDM Assistant**.

The ASDM Assistant pane appears.

Step 2 In the Search field, enter the information that you want to find, and click **Go**.

The requested information appears in the Search Results pane.

Step 3 Click any links that appear in the Search Results and Features sections to obtain more details.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

System Reload

The System Reload tool lets you schedule a system reload or cancel a pending reload.

To schedule a reload, perform the following steps:

Step 1 In the main ASDM application window, choose **Tools > System Reload**.

Step 2 In the Reload Scheduling section, define the following reload scheduling settings:

- a. For the Configuration State, choose either to save the running configuration at reload time or to discard configuration changes to the running configuration at reload time.
- b. For the Reload Start Time, you can select from the following options:
 - Click **Now** to perform an immediate reload.
 - Click **Delay by** to delay the reload by a specified amount of time. Enter the time to elapse before the reload in hours and minutes or only minutes.
 - Click **Schedule at** to schedule the reload to occur at a specific time and date. Enter the time of day the reload is to occur, and select the date of the scheduled reload.
- c. In the Reload Message field, enter a message to send to open instances of ASDM at reload time.
- d. Check the **On reload failure force immediate reload after** check box to show the amount of time elapsed in hours and minutes or only minutes before a reload is attempted again.
- e. Click **Schedule Reload** to schedules the reload as configured.

Step 3 The Reload Status area displays the status of the reload.

- Click **Cancel Reload** to stop a scheduled reload.
- Click **Refresh** to refresh the Reload Status display after a scheduled reload is finished.
- Click **Details** to display the details of a scheduled reload.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Backup and Restore

The Backup and Restore features options in the Tools menu let you back up and restore the security appliance configuration, Cisco Secure Desktop image, and SSL VPN Client images and profiles.

ASDM lets you choose the file types to back up, compresses them into a single zip file, then transfers the zip file to the directory you choose on your computer. Similarly, to restore files, you choose the source zip file on your computer and then choose the file types to be restored.

Backing Up Configurations

To back up configurations and images to a .zip file to be transferred to your local computer, perform the following steps:



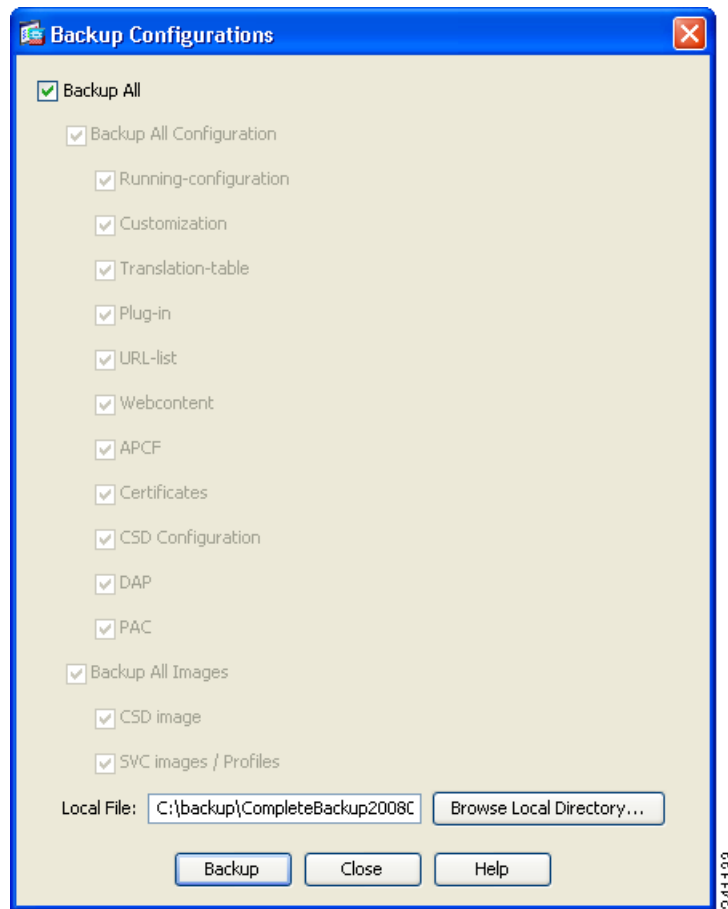
Tip

Before proceeding, create a folder on your computer to store backup files so they will be easy to find if you have to restore later.

Step 1

Choose **Tools > Backup Configurations**.

ASDM opens the Backup Configurations dialog box.



By default, all files are checked and will be backed up if they are available. If you want to back up all of the files in the list, go to Step 4.

Step 2 Uncheck the **Backup All** check box if you want to specify the configurations to back up.

Step 3 Check the options to customize the backup.

Step 4 Click **Browse Local Directory**.

The Select dialog box appears.

Step 5 Choose the path on your computer to specify the target destination for the zip file to package the backup.

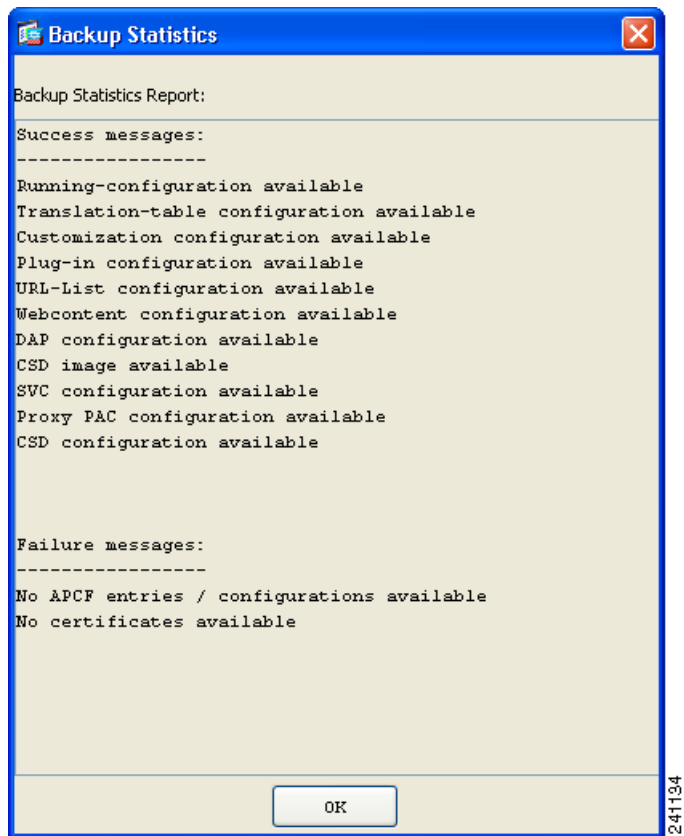
Step 6 Click **Select**.

The path appears in the Local File field.

Step 7 Enter the name of the destination backup file after the path.

Step 8 Click **Backup**.

ASDM displays a status window. When the backup completes, ASDM closes it and opens the Backup Statistics window.



This window shows the status of each backup.



Note Backup “failure messages” are most likely the consequence of no configuration present for the types indicated.

Step 9 Click **OK** to close the window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Restoring Configurations

You can specify configurations and images to restore from a zip file on your local computer. The zip file you choose must be created from the Tools > Backup Configurations option.

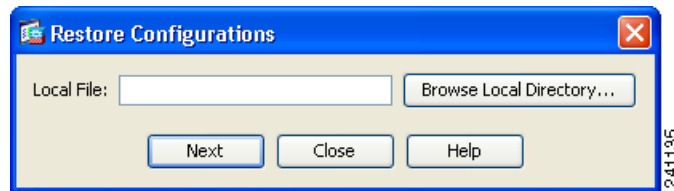
**Note**

You can only restore backups to the same security appliance from which they were originally made. Also, although you can use the Tools > Backup Configurations option to back up a running configuration, you *cannot* use the Tools > Restore Configurations option to restore it. Instead, unzip and transfer the running-config.cfg file to the security appliance file system, then use the **copy running-config.cfg startup-config** command to restore the startup configuration file. Finally, reboot to load it to memory.

To restore selected elements of the security appliance configuration, Cisco Secure Desktop image, or SSL VPN Client images and profiles, perform the following steps:

Step 1 Choose **Tools > Restore Configurations**.

The first Restore Configurations dialog box opens.

**Note**

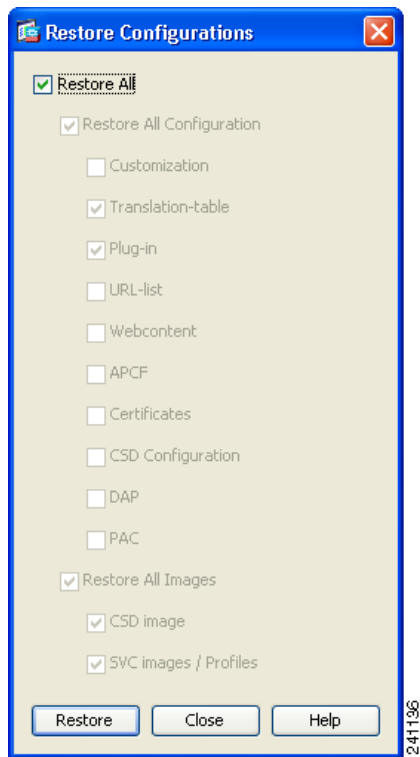
Later in the procedure, you have an opportunity to choose the configuration elements to restore; this window lets you choose the file from which to restore them.

Step 2 Click **Browse Local Directory**, choose the zip file on your local computer that contains the configuration to restore, then click **Select**.

ASDM shows the path and the zip file name in the Local File box.

Step 3 Click **Next**.

The second Restore Configuration dialog box opens.



By default, all files are checked; ASDM restores them if they are available.

Step 4 Use the default options, or uncheck them and check the specific configurations and images you want to restore.

Step 5 Click **Restore**.

ASDM displays a status window until the restore operation completes.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•



CHAPTER 4

Before You Start

This section describes the tasks you must perform before you use ASDM, and includes the following topics:

- [Factory Default Configurations, page 4-1](#)
- [Configuring the Security Appliance for ASDM Access, page 4-4](#)
- [Setting Transparent or Routed Firewall Mode at the CLI, page 4-4](#)
- [Starting ASDM, page 4-6](#)
- [Configuration Overview, page 4-9](#)

Factory Default Configurations

The factory default configuration is supported on all security appliances, except for the PIX 525 and PIX 535 models.

For the ASA 5505 model, the factory default configuration includes predefined interfaces and NAT, so that the adaptive security appliance is ready to use in your network as delivered.

For the PIX 515, PIX515E, ASA 5510, and higher version models, the factory default configuration provides a management interface to allow you to connect to the security appliance using ASDM, from which you can then complete your configuration.

The factory default configuration is available only in routed firewall mode and single context mode. See [Configuring Security Contexts](#) for more information about multiple context mode. See the [Firewall Mode Overview](#) for more information about routed and transparent firewall mode.

This section includes the following topics:

- [Restoring the Factory Default Configuration, page 4-1](#)
- [ASA 5505 Default Configuration, page 4-2](#)
- [ASA 5510 and Higher Version Default Configuration, page 4-3](#)
- [PIX 515/515E Default Configuration, page 4-4](#)

Restoring the Factory Default Configuration

To restore the factory default configuration, perform the following steps:

Step 1 Choose **File > Reset Device to the Factory Default Configuration**.

Step 2 To change the default IP address, do one of the following:

- For the ASA 5500 series, check the **Use this address for the Management 0/0 interface that will be named as “management”** check box, enter the new IP address in the Management IP Address field, and then choose the new subnet mask in the Management Subnet Mask drop-down list.
- For the PIX series, check the **Use this address for the Ethernet 1 interface, which will be named “inside”** check box, enter the new inside IP address in the Inside IP Address field, and then choose the new inside subnet mask in the Inside Subnet Mask drop-down list.

Step 3 Click **OK**.



Note

After restoring the factory default configuration, the next time you reload the adaptive security appliance, it boots from the first image in internal Flash memory. If an image does not exist in internal Flash memory, the adaptive security appliance does not boot.

ASA 5505 Default Configuration

The default factory configuration for the ASA 5505 adaptive security appliance provides the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address in the **configure factory-default** command, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside interface using PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the adaptive security appliance, so that a computer connecting to the VLAN 1 interface receives an IP address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
  switchport access vlan 2
  no shutdown
interface Ethernet 0/1
  switchport access vlan 1
  no shutdown
interface Ethernet 0/2
  switchport access vlan 1
  no shutdown
interface Ethernet 0/3
  switchport access vlan 1
  no shutdown
interface Ethernet 0/4
  switchport access vlan 1
  no shutdown
```



```
interface Ethernet 0/5
  switchport access vlan 1
  no shutdown
interface Ethernet 0/6
  switchport access vlan 1
  no shutdown
interface Ethernet 0/7
  switchport access vlan 1
  no shutdown
interface vlan2
  nameif outside
  no shutdown
  ip address dhcp setroute
interface vlan1
  nameif inside
  ip address 192.168.1.1 255.255.255.0
  security-level 100
  no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 and Higher Version Default Configuration

The default factory configuration for the ASA 5510 and higher version adaptive security appliance provides the following:

- The Management 0/0 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the adaptive security appliance, so a computer connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Default Configuration

The default factory configuration for the PIX 515/515E security appliance provides the following:

- The inside Ethernet1 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and subnet mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the security appliance, so a computer connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface ethernet 1
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Configuring the Security Appliance for ASDM Access

If you want to use ASDM instead of the CLI to configure the security appliance and you have a factory default configuration, you can connect to the default management address by pointing your browser to <https://192.168.1.1>. Alternatively, you can use the Cisco ASDM Launcher (if it is already installed) to connect to ASDM. For more information, see [Factory Default Configurations, page 4-1](#).

For the ASA 5505 adaptive security appliance, the switch port to which you connect to ASDM can be any port, except for Ethernet 0/0. On the ASA 5510 and higher version adaptive security appliances, the interface to which you connect to ASDM is Management 0/0. For the PIX 515/515E security appliance, the interface to which you connect to ASDM is Ethernet 1.

If you do not have a factory default configuration, see the *Cisco Security Appliance Command Line Configuration Guide* for instructions to access the CLI.

Setting Transparent or Routed Firewall Mode at the CLI

You can set the adaptive security appliance to run in the default routed firewall mode or transparent firewall mode. For more information about the firewall mode, see the [Firewall Mode Overview](#). For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system execution space.

When you change modes, the adaptive security appliance clears the configuration, because many commands are not supported in both modes. If you already have a populated configuration, be sure to back up this configuration before changing the mode; you can use this backup configuration for reference when you create a new configuration.

For multiple context mode, the system configuration is erased, which removes any contexts. If you again add a context that has an existing configuration that was created for the wrong mode, the context configuration will not work correctly.

**Note**

Be sure to create your context configurations for the correct mode before you add them again, or add new contexts with new paths for new configurations.

If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the adaptive security appliance changes the mode as soon as the command is executed, and then continues reading the configuration that you downloaded. If the command occurs later in the configuration, the adaptive security appliance clears all preceding lines in the configuration.

To set the firewall mode, perform the following steps.

**Note**

In multiple context mode, you must perform these steps in the system execution space.

Step 1

Make sure you back up the startup or running configuration file to use for reference before creating the new configuration. In single context mode or from the system configuration in multiple mode, you can copy the startup configuration file or running configuration file to an external server or to local Flash memory, using one of the following commands.

- To copy to a TFTP server, enter the following command:

```
hostname# copy {startup-config | running-config} tftp://server[/path]/filename
```

Where *server* is the name of the TFTP server, *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

- To copy to an FTP server, enter the following command:

```
hostname# copy {startup-config | running-config}
ftp://[user[:password]@]server[/path]/filename
```

Where *user* is your username, *password* is the password to the FTP server, *server* is the name of the FTP server, *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

- To copy to local Flash memory, enter the following command:

```
hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
disk1:/}[/path]/filename
```

Where *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

**Note**

Be sure the destination directory exists. If it does not exist, use the **mkdir** command to create the destination directory.

Step 2

To change the mode, enter one of the following commands:

- To set the mode to transparent, enter the following command:

```
hostname(config)# firewall transparent
```

This command also appears in each context configuration for information only; you cannot enter this command in a context.

- To set the mode to routed, enter the following command:

```
hostname(config)# no firewall transparent
```

Starting ASDM

This section describes how to start ASDM according to one of the following methods:

- [Downloading the ASDM Launcher, page 4-6](#)
- [Starting ASDM from the ASDM Launcher, page 4-6](#)
- [Using ASDM in Demo Mode, page 4-7](#)
- [Starting ASDM from a Web Browser, page 4-8](#)

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches more quickly, and caches previously entered IP addresses and usernames.

To download the ASDM launcher, perform the following steps:

Step 1 On the ASDM Welcome screen, click the applicable button to download the ASDM Launcher installation file.

Step 2 Double-click the **asdm-launcher.exe** file.



Note In transparent firewall mode, enter the management IP address. Be sure to enter **https**, not **http**.

Step 3 Click **OK** or **Yes** to all prompts, including the name and password prompt. Leave the name and password blank.

The installer downloads to your computer.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu. Alternatively, from the ASDM Welcome screen, you can click **Run Startup Wizard** to configure ASDM.

- Step 2** Enter or choose the adaptive security appliance IP address or hostname to which you want to connect. To clear the list of IP addresses, click the trash can icon next to the Device/IP Address/Name field.
- Step 3** Enter your username and your password, and then click **OK**.
- If there is a new version of ASDM on the adaptive security appliance, the ASDM Launcher automatically downloads the new version and requests that you update the current version before starting ASDM.
-

Using ASDM in Demo Mode

The ASDM Demo Mode, a separately installed application, lets you run ASDM without having a live device available. In this mode, you can do the following:

- Perform configuration and selected monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the CSC SSM.
- Obtain simulated monitoring and logging data, including real-time system log messages. The data shown is randomly generated; however, the experience is identical to what you would see when you are connected to a real device.

This mode does not support the following:

- Saving changes made to the configuration that appear in the GUI.
- File or disk operations.
- Historical monitoring data.
- Non-administrative users.
- These features:
 - File menu:
 - Save Running Configuration to Flash
 - Save Running Configuration to TFTP Server
 - Save Running Configuration to Standby Unit
 - Save Internal Log Buffer to Flash
 - Clear Internal Log Buffer
 - Tools menu:
 - Command Line Interface
 - Ping
 - File Management
 - Update Software
 - File Transfer
 - Upload image from Local PC
 - System Reload
 - Toolbar/Status bar > Save


- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Configuring a standby device after failover
- Operations that cause a rereading of the configuration, in which the GUI reverts to the original configuration:
 - Switching contexts
 - Making changes in the Interface pane
 - NAT pane changes
 - Clock pane changes

To run ASDM in Demo Mode, perform the following steps:

-
- Step 1** Download the ASDM Demo Mode installer, `asdm-demo-version.msi`, from one of the following locations:
- <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>
 - <http://www.cisco.com/cgi-bin/tablebuild.pl/pix>
- Step 2** Double-click the installer to install the software.
- Step 3** Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu.
- Step 4** Check the **Run in Demo Mode** check box.
- The Demo Mode window appears.
-

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

-
- Step 1** From a supported web browser on the security appliance network, enter the following URL:
- `https://interface_ip_address`
- Where `interface_ip_address` is the IP address of ASDM on the adaptive security appliance network.
- 

Note In transparent firewall mode, enter the management IP address. Be sure to enter **https**, not **http**.
-
- Step 2** Click **OK** or **Yes** to all browser prompts, including the username and password, which you should leave blank.
- The Cisco ASDM 6.0(3) Welcome page displays with the following buttons:
- **Install ASDM Launcher and Run ASDM**
 - **Run ASDM**
 - **Run Startup Wizard**
- Step 3** Click **Run ASDM**.
- Step 4** Click **OK** or **Yes** to all the browser prompts.
-

Configuration Overview

To configure and monitor the adaptive security appliance, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | For initial configuration Using the Startup Wizard , choose Wizards > Startup Wizard . |
| Step 2 | To use the IPsec VPN Wizard to configure IPsec VPN connections, choose Wizards > IPsec VPN Wizard and complete each screen that appears. |
| Step 3 | To use the SSL VPN Wizard to configure SSL VPN connections, choose Wizards > SSL VPN Wizard and complete each screen that appears. |
| Step 4 | To configure high availability and scalability settings, choose Wizards > High Availability and Scalability Wizard . See Configuring Failover with the High Availability and Scalability Wizard for more information. |
| Step 5 | To use the Packet Capture Wizard to configure packet capture, choose Wizards > Packet Capture Wizard . |
| Step 6 | To display different colors and styles available in the ASDM GUI, choose View > Office Look and Feel . |
| Step 7 | To configure features, click the Configuration button on the toolbar and then click one of the following feature buttons to display the associated configuration pane: Device Setup , Device Management , Firewall , Remote Access VPN , Site-to-Site VPN , IPS , and Trend Micro Content Security . |

**Note**

If the Configuration screen is blank, click **Refresh** on the toolbar to display the screen content.

- The Device Setup pane lets you do the following:
 - Launch the Startup Wizard to create security policy.
 - Configure basic interface parameters, including the IP address, name, security level, and the bridge group for transparent mode. For more information, see [Configuring Interfaces in Single Mode](#).
 - Configure OSPF, RIP, static, and asymmetric routing (single mode only). For more information, see [Configuring Dynamic And Static Routing](#).
 - Configure AAA services.
 - Configure digital certificates.
 - Configure the device name and device password.
 - Configure DHCP services.
 - Configure DNS services.
- The Firewall pane lets you configure security policy, including access rules, AAA rules, filter rules, service policy rules, as well as NAT rules, URL filtering servers, global objects, and perform advanced configuration for the following:
 - [Configuring Access Rules](#) determine the access of IP traffic through the security appliance. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.
 - [Ethernet Rules \(Transparent Mode Only\)](#) determine the access of non-IP traffic through the security appliance.
 - [Configuring Access Rules](#) determine authentication and/or authorization for certain types of traffic, for example, HTTP. The security appliance also sends accounting information to a RADIUS or TACACS+ server.

- [Filter Rules](#) prevent outbound access to specific websites or FTP servers. The security appliance works with a separate server running either Websense Enterprise or Sentian by N2H2. Choose **Configuration > Properties > URL Filtering** to configure the URL filtering server, which you must do before adding a rule.
- [Configuring Service Policy Rules](#) apply application inspection, connection limits, and TCP normalization. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the adaptive security appliance to do a deep packet inspection. You can also limit TCP and UDP connections, and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. An embryonic connection is a connection request that has not finished the necessary handshake between a source and destination. TCP normalization drops packets that do not appear normal.
- [NAT](#) translates addresses used on a protected network to addresses used on the public Internet. This setting lets you use private addresses, which are not routable on the Internet, on your inside networks.
- [Adding Global Objects](#) provides a single location where you can configure, view, and modify the reusable components that you need to implement your policy on the adaptive security appliance. These reusable components, or objects, include the following:
 - Network Objects/Groups
 - Service Groups
 - Class Maps
 - Inspect Maps
 - Regular Expressions
 - TCP Maps
 - Global Pools
 - Time Ranges
- The Remote Access VPN pane lets you configure network client access, clientless SSL VPN browser access and advanced web-related settings, AAA setup, certificate management, load balancing, and perform additional advanced configuration, including the following:
 - Configure IPSec connections for VPN tunnels.
 - Configure clientless SSL VPN connections. [Clientless SSL VPN](#) lets users establish a secure, remote-access VPN tunnel to the adaptive security appliance using a web browser.
 - [IKE](#) sets the IP addresses of clients after they connect through the VPN tunnel.
 - [Load Balancing](#) configures load balancing for VPN connections.
 - [E-Mail Proxy](#) configures e-mail proxies. E-mail proxies extend remote e-mail capability to clientless SSL VPN users.
- The Site-to-Site VPN pane lets you configure site-to-site VPN connections, group policies, certificate management, and perform advanced configuration, including the following:
 - [IKE Policies](#) and [IKE Parameters](#) (also called ISAKMP), which provide the negotiation protocol that lets two hosts agree on how to build an IPSec security association.
- The Device Management pane lets you configure settings to access and manage the following:
 - ASDM and HTTP over SSL management sessions.
 - FTP and TFTP clients.

- The CLI.
- SNMP and ICMP.
- Logging, including e-mail, event lists, filters, rate limit, syslog servers, and SMTP. For more information, see [Configuring Logging](#).
- User and AAA authentication.
- High availability, the Scalability Wizard, and failover.
- Advanced configuration.

**Note**

If you have a CSC SSM card or IPS software installed, either the **Trend Micro Content Security** or **IPS** feature button also appears.

- The IPS pane lets you configure the IPS sensor. For more information, see [Configuring IPS](#).
- The Trend Micro Content Security pane lets you configure the CSC SSM (available for the ASA 5500 series adaptive security appliance). For more information, see [Configuring Trend Micro Content Security](#).

Step 8

To monitor the adaptive security appliance, click the **Monitoring** button on the toolbar and then click one of the following feature buttons to display the associated monitoring pane: **Interfaces**, **VPN**, **Trend Micro Content Security**, **Routing**, **Properties**, and **Logging**.

- The Interfaces pane lets you monitor the ARP table, DHCP services, dynamic access lists, the PPOE client, connection status, and interface statistics. For more information, see [Monitoring Interfaces](#).
- The VPN pane lets you monitor VPN connections. For more information, see [Monitoring VPN](#).
- The Routing pane lets you monitor routes, OSPF LSAs, and OSPF neighbors. For more information, see [Monitoring Routing](#).
- The Properties pane lets you monitor management sessions, AAA servers, failover, CRLs, the DNS cache, and system statistics. For more information, see [Monitoring Properties](#).
- The Logging pane lets you monitor system log messages, the Real-Time Log Viewer, and the log buffer. For more information, see [Monitoring Logging](#).
- The Trend Micro Content Security pane lets you monitor CSC SSM connections. For more information, see [Monitoring Trend Micro Content Security](#).



PART 2

Device Setup and Management



CHAPTER 5

Using the Startup Wizard

The ASDM Startup Wizard guides you through the initial configuration of the adaptive security appliance, and helps you define the following settings for the adaptive security appliance:

- The hostname
- The domain name
- A password to restrict administrative access through ASDM or the CLI
- The IP address information of the outside interface
- Other interfaces, such as the inside or DMZ interfaces
- NAT or PAT rules
- DHCP settings for the inside interface, for use with a DHCP server

To access this feature from the main ASDM application window, choose one of the following:

- **Wizards > Startup Wizard.**
- **Configuration > Device Setup > Startup Wizard**, and then click **Launch Startup Wizard**.

For More Information

- See [Starting ASDM from a Web Browser](#), page 4-8.
- See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

This section includes the following topics:

- [Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances](#), page 5-2
- [Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance](#), page 5-2

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances

Table 5-1 lists all of the required Startup Wizard screens for configuring the ASA 5500 series adaptive security appliances and PIX 500 series security appliances only. The actual sequence of screens is determined by your specified configuration selections. The sequence shown applies only to the ASA 5505 adaptive security appliance. The Availability columns lists the mode or modes in which each screen appears and provides additional configuration information. Click the name to view information for the selected screen.

Table 5-1 *Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances*

Screen Name	Availability
Step 1 - Starting Point or Welcome, page 5-3	All modes. The factory default option in Step 1 is not available on the PIX security appliance.
Step 2 - Basic Configuration, page 5-4	
Step 3 - Auto Update Server, page 5-5	Single, routed and transparent modes. If enabled in single transparent mode, the Interface Configuration and Step 13 - DHCP Server screens are not available.
Step 4 - Management IP Address Configuration, page 5-6	Single, transparent mode only.
Outside Interface Configuration, page 5-22	Single, routed mode only.
Outside Interface Configuration - PPPoE, page 5-21	
Interface Configuration, page 5-20	Single, transparent mode only.
Other Interfaces Configuration, page 5-19	All modes.
Step 12 - Static Routes, page 5-13	
Step 13 - DHCP Server, page 5-13	
Step 14 - Address Translation (NAT/PAT), page 5-14	Single, routed mode only.
Step 15 - Administrative Access, page 5-15	All modes.
Step 17 - Startup Wizard Summary, page 5-19	

Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance

Table 5-2 lists all of the required Startup Wizard screens for configuring the ASA 5505 adaptive security appliance only. The sequence of screens listed represents configuration for the single, routed mode. The Availability columns lists the mode or modes in which each screen appears and provides additional configuration information. Click the name to view information for the selected screen.

Table 5-2 Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance

Screen Name and Sequence	Availability
Step 1 - Starting Point or Welcome, page 5-3	All modes. The Teleworker option in Step 2 is available only on the ASA-5505.
Step 2 - Basic Configuration, page 5-4	
Step 3 - Auto Update Server, page 5-5	Single, routed and transparent modes. Enabled only if configured for teleworker usage.
Step 4 - Management IP Address Configuration, page 5-6	Single, transparent mode only.
Step 5 - Interface Selection, page 5-6	Single, routed mode only.
Step 6 - Switch Port Allocation, page 5-7	
Step 7 - Interface IP Address Configuration, page 5-8	
Step 8 - Internet Interface Configuration - PPPoE, page 5-9	
Step 9 - Business Interface Configuration - PPPoE, page 5-10	
Step 10 - Home Interface Configuration - PPPoE, page 5-11	
Step 11 - General Interface Configuration, page 5-12	
Step 12 - Static Routes, page 5-13	All modes. Enabled only if configured for teleworker usage.
Step 13 - DHCP Server, page 5-13	All modes.
Step 14 - Address Translation (NAT/PAT), page 5-14	Single, routed mode only.
Step 15 - Administrative Access, page 5-15	All modes.
Step 16 - Easy VPN Remote Configuration, page 5-17	Single, routed mode, only when enabled for teleworker usage.
Step 17 - Startup Wizard Summary, page 5-19	All modes.

Step 1 - Starting Point or Welcome

To access this feature from the main ASDM application window (except in multiple mode), choose **File > Reset Device to the Factory Default Configuration**.

Fields

- Modify existing configuration—Choose this option to change the existing configuration.
- Reset configuration to factory defaults—Choose this option to set the configuration at the factory default values for the inside interface.
- Configure the IP address of the management interface—Check this check box to configure the IP address and subnet mask of the management interface.
- IP Address—Specifies the IP address of the management interface.
- Subnet Mask—Choose the subnet mask of the management interface from the drop-down list.

**Note**

If you reset the configuration to factory defaults, you cannot undo these changes by clicking **Cancel** or by closing this screen.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Step 2 - Basic Configuration

To access this feature from the main ASDM application window, choose one of the following:

- **Configuration > Properties > Device Administration > Device**
- **Configuration > Properties > Device Administration > Password**

Fields

- Configure the device for Teleworker usage—Check this check box to specify a group of configuration settings for a remote worker. For more information, see [Step 16 - Easy VPN Remote Configuration, page 5-17](#).
- Host Name—Specifies a hostname for the adaptive security appliance. The hostname can be up to 63 alphanumeric characters in mixed case. Either “ASA” or “PIX” appears as the device type, according to the security appliance you are using.
- Domain Name—Specifies the IPSec domain name of the adaptive security appliance, which can be used for certificates. The domain name can be a maximum of 63 alphanumeric characters, with no special characters or spaces.
- Privileged Mode (Enable) Password area—Allows you to restrict administrative access to the adaptive security appliance through ASDM or the CLI.

**Note**

If you leave the password field blank, a Password Confirmation dialog box appears to notify you that to do so is a high security risk.

- Change privileged mode (enable) password—Check this check box to change the current privileged mode (enable) password.
- Old Password—Specifies the old enable password, if one exists.
- New Password—Specifies the new enable password. The password is case-sensitive and can be up to 32 alphanumeric characters.
- Confirm New Password—Lets you reenter the new enable password.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Step 3 - Auto Update Server

This screen allows you to manage the adaptive security appliance remotely from an Auto Update Server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- **Enable Auto Update**—Check this check box to enable communication between the security appliance and an Auto Update Server.
- **Server URL**—From the drop-down list, choose either HTTPS or HTTP to define the beginning of the URL for the Auto Update Server.
- **Verify Server SSL certificate**—Check this check box to confirm that an SSL certificate is enabled on the Auto Update Server.
- **Username**—Specifies the username to log in to the Auto Update Server.
- **Password**—Specifies the password to log in to the Auto Update Server.
- **Confirm Password**—Reenter the password to confirm it.
- **Device ID Type**—Choose the type of ID from the drop-down list to uniquely identify the adaptive security appliance. Choose **User-defined name** to enable the Device ID field, where you specify a unique ID.
- **Device ID**—Specifies a unique string to use as the adaptive security appliance ID.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Step 4 - Management IP Address Configuration

This screen lets you configure the management IP address of the host for this context. To access this feature from the main ASDM application window, choose **Configuration > Properties > Management IP**.

Fields

- **Management IP Address**—Specifies the IP address of the host that can access this context for management purposes using ASDM or a session protocol.
- **Subnet Mask**—Specifies the subnet mask for the Management IP address.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	—	—	—

Step 5 - Interface Selection

This screen allows you to group the eight, Fast Ethernet switch ports on the ASA 5505 into three VLANs. These VLANs function as separate, Layer 3 networks. You can then choose or create the VLANs that define your network—one for each interface: outside (Internet), inside (Business), or DMZ (Home). A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

Fields

Outside VLAN or Internet VLAN area

- **Choose a VLAN**—Choose a predefined outside VLAN by number from the drop-down list.
- **Create a VLAN**—Check this check box to create a new outside VLAN.
- **Enable VLAN**—Check this check box to enable the outside VLAN.

Inside VLAN or Business VLAN area

- **Choose a VLAN**—Choose a predefined inside VLAN by number from the drop-down list.
- **Create a VLAN**—Check this check box to create a new inside VLAN.
- **Enable VLAN**—Check this check box to enable the inside VLAN.

DMZ VLAN or Home VLAN (Optional) area

- **Choose a VLAN**—Choose a predefined VLAN by number from the drop-down list.
- **Create a VLAN**—Check this check box to create a new VLAN.

- Do not configure—Check this check box to disable configuration of this VLAN.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 6 - Switch Port Allocation

This screen lets you allocate switch ports to outside (Internet), inside (Business), or DMZ (Home) interfaces. The DMZ interface is not available in transparent mode. You must add the ports to the associated VLANs. By default, all switch ports begin with VLAN1. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

Switch Ports for Outside VLAN (*vlanid*) or Switch Ports for Internet VLAN (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

Switch Ports for Inside VLAN (*vlanid*) or Switch Ports for Business VLAN (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

Switch Ports for DMZ VLAN (*vlanid*) or Switch Ports for Home VLAN (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 7 - Interface IP Address Configuration

This screen allows you to configure the interface by obtaining an IP address from a PPPoE server or a DHCP server, or by specifying an IP address and subnet mask.

Fields

Outside IP Address or Internet IP Address area

- Use the following IP address—Choose this option to specify an outside IP address.
- IP Address/ Mask—Enter the specific IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain an outside IP address from a DHCP server.
- Obtain default route using DHCP—Check this check box to obtain the default route for an outside IP address from a DHCP server.
- Use PPoE—Choose this option to obtain an outside IP address from a PPoE server.

Inside IP Address or Business IP Address area

- Use the following IP address—Choose this option to specify an inside IP address.
- IP Address/ Mask—Enter the specific inside IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain an inside IP address from a DHCP server.
- Use PPoE—Choose this option to obtain an inside IP address from a PPoE server.

DMZ IP Address or Home IP Address area

- Use the following IP address—Choose this option to specify a DMZ IP address.
- IP Address/ Mask—Enter the specific DMZ IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain a DMZ IP address from a DHCP server.
- Use PPoE—Choose this option to obtain a DMZ IP address from a PPoE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 8 - Internet Interface Configuration - PPPoE

This screen lets you configure the specified outside interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.



Note

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- **Group Name**—Specifies the name of your group on the PPPoE server. You must specify a group name to proceed.

User Authentication area

- **PPPoE Username**—Specifies your username on the PPPoE server.
- **PPPoE Password**—Specifies your password on the PPPoE server.
- **Confirm PPPoE Password**—Specifies the PPPoE password you originally entered.

Authentication Method area

- **PAP**—Click to use PAP authentication.
- **CHAP**—Click to use CHAP authentication.
- **MSCHAP**—Click to use MSCHAP authentication.

IP Address area

- **Obtain an IP address using PPPoE**—Choose this option to obtain an IP address for the interface from the PPPoE server. This field is not visible in transparent mode.
- **Specify an IP Address**—Specifies an IP address for the Internet interface. This field is not visible in transparent mode.
 - **IP Address**—Specifies the IP address that you want to use for the Internet interface.
 - **Subnet Mask**—Choose a subnet mask for the Internet interface from the drop-down list.
- **Obtain default route using PPPoE**—Check this check box to set the default routing using the PPPoE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 9 - Business Interface Configuration - PPPoE

This screen lets you configure the inside interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.



Note

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- **Group Name**—Specifies the name of your group on the PPPoE server. You must specify a group name to proceed.

User Authentication area

- **PPPoE Username**—Specifies your username on the PPPoE server.
- **PPPoE Password**—Specifies your password on the PPPoE server.
- **Confirm PPPoE Password**—Specifies the PPPoE password you originally entered.

Authentication Method area

- **PAP**—Click to use PAP authentication.
- **CHAP**—Click to use CHAP authentication.
- **MSCHAP**—Click to use MSCHAP authentication.

IP Address area

- **Obtain an IP address using PPPoE**—Choose this option to obtain an IP address for the interface from the PPPoE server. This field is not visible in transparent mode.
- **Specify an IP Address**—Specifies an IP address for the inside interface. This field is not visible in transparent mode.
 - **IP Address**—Specifies the IP address that you want to use for the inside interface.
 - **Subnet Mask**—Choose a subnet mask for the Internet interface from the drop-down list.
- **Obtain default route using PPPoE**—Check this check box to set the default routing using the PPPoE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 10 - Home Interface Configuration - PPPoE

This screen lets you configure the DMZ interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

**Note**

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- **Group Name**—Specifies the name of your group on the PPPoE server. You must specify a group name to proceed.

User Authentication area

- **PPPoE Username**—Specifies your username on the PPPoE server.
- **PPPoE Password**—Specifies your password on the PPPoE server.
- **Confirm PPPoE Password**—Specifies the PPPoE password you originally entered.

Authentication Method area

- **PAP**—Click to use PAP authentication.
- **CHAP**—Click to use CHAP authentication.
- **MSCHAP**—Click to use MSCHAP authentication.

IP Address area

- **Obtain an IP address using PPPoE**—Choose this option to obtain an IP address for the interface from the PPPoE server. This field is not visible in transparent mode.
- **Specify an IP Address**—Specifies an IP address for the DMZ interface. This field is not visible in transparent mode.
 - **IP Address**—Specifies the IP address that you want to use for the DMZ interface.
 - **Subnet Mask**—Choose a subnet mask for the Internet interface from the drop-down list.

- Obtain default route using PPPoE—Check this check box to set the default routing using the PPPoE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 11 - General Interface Configuration

This screen lets you enable and restrict traffic between interfaces and between hosts connected to the same interface.

Restricted traffic is not an optional configuration. If you only have a restricted license, you must restrict traffic from one interface to any of the other interfaces. The Restrict Traffic area fields are hidden if you have a full license or if the device is in transparent mode.

Fields

- Enable traffic between two or more interfaces with the same security level—Check this check box to enable traffic between two or more interfaces with the same security level.
- Enable traffic between two or more hosts connected to the same interface—Check this check box to enable traffic between two or more hosts connected to the same interface.

Restrict traffic area

- From interface—Lets you restrict traffic from an interface by choosing an interface from the drop-down list.
- To interface—Lets you restrict traffic to an interface by choosing an interface from the drop-down menu.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 12 - Static Routes

This screen lets you create, edit, and remove static routes that will access networks connected to a router on any interface.

For More Information

- [Static Routes, page 11-40](#)
- [Add/Edit Static Routes, page 5-13](#)
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Static Routes

This dialog box lets you add or edit a static route. See [Add/Edit Static Route, page 11-43](#) for more information.

Step 13 - DHCP Server

This screen lets you configure the adaptive security appliance as a DHCP server to hosts on the inside interface. To configure the DHCP server for other interfaces from the main ASDM application window, choose **Configuration > Properties > DHCP Services > DHCP Server**. For more information, see [DHCP Server, page 13-4](#).

Fields

- Enable DHCP server on the inside interface—Check this check box to allow connection to the DHCP server from the inside interface.

DHCP Address Pool area

- Starting IP Address—Specifies the starting range of the DHCP server pool in a block of IP addresses from the lowest to highest.



Note

The adaptive security appliance supports up to 256 IP addresses.

- Ending IP Address—Specifies the ending range of the DHCP server pool in a block of IP addresses from the lowest to highest.

DHCP Parameters area

- Enable auto-configuration—Check this check box to allow automatic configuration of the DNS server, WINS server, lease length, and ping timeout settings.
- DNS Server 1—Specifies the IP address of the DNS server.
- WINS Server 1—Specifies the IP address of the WINS server.
- DNS Server 2—Specifies the IP address of the alternate DNS server.
- WINS Server 2—Specifies the IP address of the alternate WINS server.
- Lease Length (secs)—Specifies the amount of time (in seconds) that the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
- Ping Timeout—Specifies the parameters for the ping timeout value in milliseconds.
- Domain Name—Specifies the domain name of the DNS server to use DNS.
- Enable auto-configuration from interface—Check this check box to enable DHCP auto-configuration and choose the interface from the menu. The values you specify in the previous areas of this pane take precedence over the auto-configured values.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Step 14 - Address Translation (NAT/PAT)

This screen lets you configure NAT and PAT on your security appliance. To access this feature from the main ASDM application window, choose **Configuration > NAT**.

PAT lets you set up a single IP address for use as the global address. In addition, you can set multiple outbound sessions to appear as if they originate from a single IP address. PAT lets up to 65,535 hosts start connections through a single outside IP address.

If you decide to use NAT, enter an address range to use for translating all addresses on the inside interface to addresses on the outside interface. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound connections resulting from outbound connections.

When you use PAT, be aware of the following:

- PAT does not work with caching name servers.
- You may need to enable the corresponding inspection engine to pass multimedia application protocols through the security appliance.
- PAT does not work with the **established** command.
- With passive FTP, use the **inspect protocol ftp strict** command with the **access-list** command to allow outbound FTP traffic.

- A DNS server on a higher level security interface cannot use PAT.

Fields

- Use Network Address Translation (NAT)—Choose to enable NAT and a range of IP addresses to be used for translation.
- Starting Global IP Address—Specifies the first IP address in a range of IP addresses to be used for translation.
- Ending Global IP Address—Specifies the last IP address in a range of IP addresses to be used for translation.
- Subnet Mask (optional)—Specify the subnet mask for the range of IP addresses to be used for translation.
- Use Port Address Translation (PAT)—Choose to enable PAT. Choose one of the following if you select this option:



Note IPSec with PAT may not work correctly, because the outside tunnel endpoint device cannot handle multiple tunnels from one IP address.

- Use the IP address on the outside interface—Choose to use the IP address of the outside interface for PAT.
- Specify an IP address—Enter an IP address to be used for PAT.

IP Address—Specifies an IP address for the outside interface for PAT.

Subnet Mask (optional)—Choose a subnet mask from the drop-down list.

- Enable traffic through the firewall without translation—Choose to allow traffic through the firewall without translation.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 15 - Administrative Access

This screen lets you configure management access on the security appliance.

Fields

- Type—Specifies whether the host or network is accessing the security appliance through HTTP over SSL in ASDM, SSH, or Telnet.

- **Interface**—Displays the host or network name.
- **IP Address**—Displays the IP address of the host or network.
- **Mask**—Displays the subnet mask of the host or network.
- **Enable HTTP server for HTTPS/ASDM access**—Check this check box to enable a secure connection to an HTTP server to access ASDM.
- **Add**—Click to add the access type, an interface, and then specifies the IP address and netmask of the host network that may connect to that interface for management purposes only. See [Add/Edit Administrative Access Entry](#) for more information.
- **Edit**—Changes an interface. See [Add/Edit Administrative Access Entry](#) for more information.
- **Delete**—Removes an interface.
- **Enable ASDM history metrics**—Check this check box to allow ASDM to collect and display statistics.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Administrative Access Entry

This dialog box let you configure the hosts. To access this feature from the main ASDM application window, choose one of the following:

- **Configuration > Properties > Device Access > HTTPS/ASDM**
- **Configuration > Properties > Device Access > Telnet**
- **Configuration > Properties > Device Access > SSH**
- **Configuration > Properties > History Metrics**

Fields

- **Access Type**—Choose one of the following types of preconfigured connections for the CLI console sessions from the drop-down list:
 - ASDM/HTTPS
 - SSH
 - Telnet



Note

ASDM uses HTTP over SSL for all communication with the security appliance.

- Interface Name—Choose from a list of predetermined interfaces.
- IP Address—Specifies an IP address for the interface.
- Subnet Mask—Specifies a subnet mask for the interface from a selection of subnet mask IP addresses.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Step 16 - Easy VPN Remote Configuration

This screen lets you form a secure VPN tunnel between the adaptive security appliance and a remote Cisco VPN 3000 concentrator, Cisco router, or adaptive security appliance that is acting as an Easy VPN server. The adaptive security appliance acts as an Easy VPN remote device to enable deployment of VPNs to remote locations.



Note

To access this screen, you must check the **Configure the device for Teleworker usage** check box in [Step 2 - Basic Configuration](#) and uncheck the **Enable Auto Update** check box in the [Interface Configuration](#).

Two modes of operation are available:

- Client mode
- Network extension mode

In client mode, the adaptive security appliance does not expose the IP addresses of clients on the inside network. Instead, the adaptive security appliance uses NAT to translate the IP addresses on the private network to a single, assigned IP address. In this mode, you cannot ping or access any device from outside the private network.

In extension mode, the adaptive security appliance does not protect the IP addresses of local hosts by substituting an assigned IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

To configure the adaptive security appliance in one of these two modes, use the following guidelines:

Use client mode if:

- You want VPN connections to be initiated by client traffic.
- You want the IP addresses of local hosts to be hidden from remote networks.
- You are using DHCP on the ASA 5505 to provide IP addresses to local hosts.

Use network extension mode if:

- You want VPN connections to remain open even when not required for transmitting traffic.
- You want remote hosts to be able to communicate directly with hosts on the local network.
- Hosts on the local network have static IP addresses.

Fields

- Enable Easy VPN remote—Check this check box to enable the adaptive security appliance to act as an Easy VPN remote device. If you do not enable this feature, any host that has access to the adaptive security appliance outside interface through a VPN tunnel can manage it remotely.

Mode area

- Client mode—Click if you are using a DHCP server to generate dynamic IP addresses for hosts on your inside network.
- Network Extension—Click if hosts on your inside network have static IP addresses.

Group Settings area

- Use X.509 Certificate—Click to use X.509 certificates to enable the IPsec main mode. Choose or enter the trustpoint from the drop-down list.
- Use group password—Lets you enter a password for a group of users.
 - Group Name—Lets you enter a name for the user group.
 - Password—Lets you enter a password for the user group.
 - Confirm password—Requires that you confirm the password.

User Settings area

- Username—Lets you enter a username for your settings.
- Password—Lets you enter a password for your settings.
- Confirm Password—Requires that you confirm the password for your settings.

Easy VPN Server area

- Primary server—Lets you enter the IP address of the primary Easy VPN server.
- Secondary server—Lets you enter the IP address of a secondary Easy VPN server.

**Note**

The adaptive security appliance supports a maximum of 11 Easy VPN servers: one primary and up to ten secondary. Before you can connect the ASA Easy VPN remote device to the Easy VPN server, you must establish network connectivity between both devices through your ISP. After you have connected the ASA 5500 series adaptive security appliance to the DSL or cable modem, follow the instructions provided by your ISP to complete the network connection. You can obtain an IP address through a PPPoE server, a DHCP server, or a static configuration.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Step 17 - Startup Wizard Summary

This screen summarizes all of the settings you have made for the security appliance.

- To change any of the settings in previous screens, click **Back**.
- If you started the Startup Wizard directly from a browser, when you click **Finish**, the configuration that you created through the wizard is sent to the adaptive security appliance and saved in flash memory automatically.
- If you ran the Startup Wizard from within ASDM, you must explicitly save the configuration in Flash memory.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Other Interfaces Configuration

This screen lets you configure the remaining interfaces.

Fields

- Interface—Displays the network interface on which the original host or network resides.
- Name—Displays the name of the interface being configured.
- Security Level—Displays the security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- Enable traffic between two or more interfaces with same security levels—Check this check box to assign the same security level to two or more interfaces, and enable traffic between them.
- Enable traffic between two or more hosts connected to the same interface—Check this check box if you have an interface between two or more hosts and want to enable traffic between them.
- Edit—Click to change the configuration of the interface in the [Edit Interface](#) dialog box.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit Interface

To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- Interface—Displays the name of the selected interface to edit.
- Interface Name—Displays the name of the selected interface, and lets you change the name of the interface.
- Security Level—Displays the security level of the selected interface, or lets you select a security level for the interface. If you change the security level of the interface to a lower level, a warning message appears.
- Use PPPoE—Check this check box to use PPPoE to provide an authenticated method of assigning an IP address to an outside interface.



Note

Because PPPoE is permitted on multiple interfaces, each instance of the PPPoE client may require different authentication levels with different usernames and passwords.

- Use DHCP—Check this check box to use the adaptive security appliance as a DHCP server.
- Uses the following IP address—Check this check box to enter a specific IP address for an interface.
- IP Address—Edits the IP address of the interface.
- Subnet Mask—Choose an existing subnet mask from the drop-down list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Interface Configuration

This screen lets you configure the remaining interfaces and enable traffic between two or more interfaces.

Fields

- Edit—Click to change the configuration of the interface in the [Edit Interface](#) dialog box.

- Enable traffic between two or more interfaces with the same security level—Check this check box to enable traffic between two or more interfaces with the same security level.

**Note**

IP address-related fields are not available in transparent mode.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

Outside Interface Configuration - PPPoE

This screen lets you configure the outside interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- Group Name—Lets you specify the name of the interface. You must specify a group name to proceed.
- User Authentication area
 - PPPoE Username—Lets you specify the PPPoE username for authentication purposes.
 - PPPoE Password—Lets you specify the PPPoE password for authentication purposes.
 - Confirm PPPoE Password—Lets you confirm the PPPoE password.
- Authentication Method area

The default authentication method for PPPoE is PAP. You have the option of configuring CHAP or MS-CHAP manually.

- PAP—Check this check box to select PAP as the authentication method. The username and password are sent unencrypted using this method.
- CHAP—Check this check box to select CHAP authentication. CHAP does not prevent unauthorized access; it identifies the remote end. The access server then determines whether the user is allowed access.
- MSCHAP—Check this check box to select MS-CHAP authentication for PPP connections between a computer using a Windows operating system and an access server.
- IP Address area

The default authentication method for PPPoE is PAP. You have the option of configuring CHAP or MS-CHAP manually.

 - Obtain IP Address using PPPoE—Click to obtain an IP address using a PPPoE server.

- Specify an IP address—Click to specify an IP address for an interface:
 IP Address—Lets you enter an IP address for an interface.
 Subnet Mask—Lets you enter or choose a subnet mask for an interface from the drop-down list.
- Obtain default route using PPPoE—Click to obtain the default route between the PPPoE server and the PPPoE client.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—

Outside Interface Configuration

This screen lets you configure your outside interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.



Note

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- Interface—Choose an interface from the drop-down list.
- Interface Name—Adds a name to a new interface, or displays the name associated with an existing interface.
- Enable interface—Check this check box to activate the interface in privileged mode.
- Security Level—Displays the security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- Use PPPoE—Click to obtain an IP address from a PPPoE server.
- Use DHCP—Click to obtain an IP address from a DHCP server.
- Obtain default route using DHCP—Check this check box to obtain an IP address for the default gateway using DHCP.

- Use the following IP address—Choose this option to specify an IP address manually for the interface. This field is not visible in transparent mode.
- IP Address—Specifies an IP address for an outside interface. This field is not visible in transparent mode.
- Subnet Mask—Choose a subnet mask for an outside interface from the drop-down list.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	•	—



CHAPTER 6

Configuring Basic Device Settings

This section contains the following topics:

- [Management IP Address, page 6-1](#)
- [System Time, page 6-2](#)
- [Configuring Advanced Device Management Features, page 6-4](#)
- [System Image/Configuration, page 6-6](#)
- [Device Name/Password, page 6-12](#)
- [System Software, page 6-13](#)

Management IP Address

The Management IP pane lets you set the management IP address for the security appliance or for a context in transparent firewall mode. A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is the management IP address. The exception is that you can set the IP address for the Management 0/0 management-only interface, which does not pass through traffic. See the [Configuring Interfaces in Single Mode](#) chapter to set the IP address for Management 0/0.

This address is required, because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access.

Fields

- Management IP Address—Sets the management IP address.
- Subnet Mask—Sets the subnet mask.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

System Time

You can manually set the system date or time or have the security appliance dynamically set the system date and time using an NTP server.

See the following topics for more information:

- [Clock, page 6-2](#)
- [NTP, page 6-3](#)

Clock

The Clock pane lets you manually set the date and time for the security appliance. The time displays in the status bar at the bottom of the main ASDM pane.

In multiple context mode, you can set the time in the system configuration only.

To dynamically set the time using an NTP server, see the [NTP](#) pane; time derived from an NTP server overrides any time set manually in the [Clock](#) pane.

Fields

- **Time Zone**—Sets the time zone as GMT plus or minus the appropriate number of hours. If you select the Eastern Time, Central Time, Mountain Time, or Pacific Time zone, then the time adjusts automatically for daylight savings time, from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

**Note**

Changing the time zone on the security appliance may drop the connection to intelligent SSMs.

- **Date**—Sets the date. Click the Date drop-down list to display a calendar. Then navigate to the correct date using the following methods:
 - Click the name of the month to display a list of months. Click the desired month. The calendar updates to that month.
 - Click the year to change the year. You can use the up and down arrows to scroll through the years, or you can type a year in the entry field.
 - Click the arrows to the right and left of the month and year display to scroll the calendar forward and backwards one month at a time.
 - Click a day on the calendar to set the date.
- **Time**—Sets the time on a 24-hour clock.
 - hh, mm, and ss boxes—Sets the hour, minutes, and seconds.
- **Update Display Time**—Updates the time shown in the bottom right corner of the ASDM pane. The current time updates automatically every ten seconds.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

NTP

The NTP pane lets you define NTP servers to dynamically set the time on the security appliance. The time displays in the status bar at the bottom of the main ASDM pane.

Time derived from an NTP server overrides any time set manually in the [Clock](#) pane.

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The security appliance chooses the server with the lowest stratum—a measure of how reliable the data is.

Fields

- NTP Server List—Shows defined NTP servers.
 - IP Address—Shows the NTP server IP address.
 - Interface—Specifies the outgoing interface for NTP packets, if configured. The system does not include any interfaces, so it uses the admin context interfaces. If the interface is blank, then the security appliance uses the default admin context interface according to the routing table.
 - Preferred?—Shows whether this NTP server is a preferred server, Yes or No. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. For example, the security appliance uses a more accurate server over a less accurate server that is preferred.
 - Key Number—Shows the authentication key ID number.
 - Trusted Key?—Shows if the key is a trusted key, Yes or No. The key must be trusted for authentication to work.
- Enable NTP Authentication—Enables authentication for all servers.
- Add—Adds an NTP server.
- Edit—Edits an NTP server.
- Delete—Deletes and NTP server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Add/Edit NTP Server Configuration

The Add/Edit NTP Server Configuration dialog box lets you add or edit an NTP server.

Fields

- **IP Address**—Sets the NTP server IP address.
- **Preferred**—Sets this server as a preferred server. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. For example, the security appliance uses a more accurate server over a less accurate server that is preferred.
- **Interface**—Sets the outgoing interface for NTP packets, if you want to override the default interface according to the routing table. The system does not include any interfaces, so it uses the admin context interfaces. If you intend to change the admin context (thus changing the available interfaces), you should choose **None** (the default interface) for stability.
- **Authentication Key**—Sets the authentication key attributes if you want to use MD5 authentication for communicating with the NTP server.
 - **Key Number**—Sets the key ID for this authentication key. The NTP server packets must also use this key ID. If you previously configured a key ID for another server, you can select it in the list; otherwise, type a number between 1 and 4294967295.
 - **Trusted**—Sets this key as a trusted key. You must select this box for authentication to work.
 - **Key Value**—Sets the authentication key as a string up to 32 characters in length.
 - **Reenter Key Value**—Validates the key by ensuring that you enter the key correctly two times.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Configuring Advanced Device Management Features

The following sections describe how to configure the items in the Advanced section.

Configuring HTTP Redirect

The HTTP Redirect table displays each interface on the security appliance, shows whether it is configured to redirect HTTP connections to HTTPS, and the port number from which it redirects those connections.

**Note**

To redirect HTTP, the interface requires an access list that permits HTTP. Otherwise, the interface cannot listen to the HTTP port.

To change the HTTP redirect setting of an interface or the port from which it redirects HTTP connections, select the interface in the table and click **Edit**. You can also double-click an interface. The Edit HTTP/HTTPS Settings dialog box opens.

Edit HTTP/HTTPS Settings

The Edit HTTP/HTTPS Settings dialog box lets you change the HTTP redirect setting of an interface or the port number.

Fields

The Edit HTTP/HTTPS Settings dialog box includes the following fields:

- **Interface**—Identifies the interface on which the security appliance redirects or does not redirect HTTP requests to HTTPS.
- **Redirect HTTP to HTTPS**—Check to redirect HTTP requests to HTTPS, or uncheck to not redirect HTTP requests to HTTPS.
- **HTTP Port**—Identifies the port from which the interface redirects HTTP connections. By default it listens to port 80.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Maximum SSL VPN Sessions

This pane lets you set a maximum number of SSL VPN sessions.

Fields

Maximum Sessions—Enter the maximum number of Clientless SSL VPN sessions you want to allow. Be aware that the different ASA models support Clientless SSL VPN sessions as follows: ASA 5510 supports a maximum of 250; ASA 5520 maximum is 750; ASA 5540 maximum is 2500; ASA 5550 maximum is 5000.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

History Metrics

The History Metrics pane lets you configure the adaptive security appliance to keep a history of various statistics, which ASDM can display on any Graph/Table. If you do not enable history metrics, you can only monitor statistics in real time. Enabling history metrics lets you view statistics graphs from the last 10 minutes, 60 minutes, 12 hours, and 5 days.

To configure history metrics, perform the following steps:

-
- Step 1** Choose **Configuration > Device Management > Advanced > History Metrics**.
- The History Metrics pane appears.
- Step 2** Check the **ASDM History Metrics** check box to enable history metrics, and then click **Apply**.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Image/Configuration

This section includes the following topics:

- [Activation Key, page 6-6](#)
- [Auto Update, page 6-7](#)
- [Boot Image/Configuration, page 6-10](#)

Activation Key

Software licenses and their features are activated by activation keys. The Activation Key pane lets you view the device serial number and activation keys in the running configuration and flash memory. You can also update the activation key on this pane.

Features of temporary and permanent licenses combine to form the running license. When you activate a temporary license, it overrides any previously-activated temporary license and combines with the permanent license to create a new running license. When you activate a permanent license, it overwrites the currently running permanent and temporary licenses and becomes the running license.

The security appliance displays any resolved conflicts between the temporary and permanent licenses when you enter a temporary activation-key.

To update the activation key, perform the following steps:

Step 1 Go to **Configuration > Device Management > System Image/Configuration > Activation Key**.

Step 2 Enter the new activation key in the New Activation Key field. Enter the activation key as a four- or five-element hexadecimal string with one space between each element, for example:

0x00000000 0x00000000 0x00000000 0x00000000

The leading 0x specifier is optional; all values are assumed to be hexadecimal. The key is not stored in the configuration file. The key is tied to the serial number.

Step 3 Click **Update Activation Key**.

Auto Update

The Auto Update pane lets you configure the security appliance to be managed remotely from servers that support the Auto Update specification. Auto Update lets you apply configuration changes to the security appliance and receive software updates from remote locations.

Auto Update is useful in solving many of the challenges facing administrators for security appliance management:

- Overcomes dynamic addressing and NAT challenges.
- Gives ability to commit configuration changes in one atomic action.
- Provides a reliable method for updating software.
- Leverages well understood methods for high scalability.
- Open interface gives developers tremendous flexibility.
- Simplifies security solutions for Service Provider environments.
- High reliability, rich security/management features, broad support by many products.

The Auto Update specification provides the infrastructure necessary for remote management applications to download security appliance configurations, software images, and to perform basic monitoring from a centralized location or multiple locations.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time. Communication between the Auto Update server and the security appliance requires a communications path and local CLI configuration on each security appliance.

The Auto Update feature on the security appliance can be used with Cisco security products, as well as products from third-party companies that want to manage the security appliance.

Important Notes

- If the security appliance configuration is updated from an Auto Update server, ASDM is not notified. You must choose **Refresh** or **File > Refresh ASDM with the Running Configuration on the Device** to get the latest configuration, and any changes to the configuration made in ASDM will be lost.
- If HTTPS is chosen as the protocol to communicate with the Auto Update server, the security appliance will use SSL. This requires the security appliance to have a DES or 3DES license.

Fields

The Auto Update pane consists of an Auto Update Servers table and two areas: the Timeout area, and the Polling area.

The Auto Update Servers table lets you view the parameters of previously-configured Auto Update servers. The security appliance polls the server listed at the top of the table first. You can change the order of the servers in the table with the Move Up and Move Down buttons. The Auto Update Servers table contains the following columns:

- **Server**—The name or IP address of the Auto Update server.
- **User Name**—The user name used to access the Auto Update server.
- **Interface**—The interface used when sending requests to the Auto Update server.
- **Verify Certificate**—Indicates whether the security appliance checks the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the security appliance use the same CA.

Double-clicking any of the rows in the Auto Update Server table opens the Edit Auto Update Server dialog box, in which you can modify the Auto Update server parameters. These changes are immediately reflected in the table, but you must click **Apply** to save them to the configuration.

The Timeout area lets you set the amount of time the security appliance waits for the Auto Update server to time out. The Timeout area contains the following fields:

- **Enable Timeout Period**—Check to enable the security appliance to time out if no response is received from the Auto Update server.
- **Timeout Period (Minutes)**—Enter the number of minutes the security appliance will wait to time out if no response is received from the Auto Update server.

The Polling area lets you configure how often the security appliance will poll for information from the Auto Update server. The Polling area contains the following fields:

- **Polling Period (minutes)**—The number of minutes the security appliance will wait to poll the Auto Update server for new information.
- **Poll on Specified Days**—Allows you to specify a polling schedule.
- **Set Polling Schedule**—Displays the Set Polling Schedule dialog box where you can configure the days and time-of-day to poll the Auto Update server.
- **Retry Period (minutes)**—The number of minutes the security appliance will wait to poll the Auto Update server for new information if the attempt to poll the server fails.
- **Retry Count**—The number of times the security appliance will attempt to retry to poll the Auto Update server for new information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Set Polling Schedule

The Set Polling Schedule dialog box lets you configure specific days, and the time-of-day for the security appliance to poll the Auto Update server.

Fields

The Set Polling Schedule dialog box contains the following fields:

Days of the Week—Check the days of the week that you want the security appliance to poll the Auto Update server.

The Daily Update pane group lets you configure the time of day when you want the security appliance to poll the Auto Update server, and contains the following fields:

- **Start Time**—Enter the hour and minute to begin the Auto Update poll.
- **Enable randomization**—Check to enable the security appliance to randomly choose a time to poll the Auto Update server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Auto Update Server

The Edit Auto Update Server dialog box contains the following fields:

- **URL**—The protocol the Auto Update server uses to communicate with the security appliance, either http or https, and the path to the Auto Update server.
- **Interface**—The interface to use when sending requests to the Auto Update server.
- **Verify Certificate**—Select to enable the security appliance to verify the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the security appliance use the same CA.

The User area contains the following fields:

- **User Name (Optional)**—Enter the user name needed to access the Auto Update server.
- **Password**—Enter the user password for the Auto Update server.
- **Confirm Password**—Reenter the user password for the Auto Update server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Advanced Auto Update Settings

Fields

- Use Device ID to uniquely identify the ASA—Enables authentication using a Device ID. The Device ID is used to uniquely identify the security appliance to the Auto Update server.
- Device ID—Type of Device ID to use.
 - Hostname—The name of the host.
 - Serial Number—Device serial number.
 - IP Address on interface—The IP address of the selected interface, used to uniquely identify the security appliance to the Auto Update server.
 - MAC Address on interface—The MAC address of the selected interface, used to uniquely identify the security appliance to the Auto Update server.
 - User-defined value—A unique user ID.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Boot Image/Configuration

Boot Image/Configuration lets you choose which image file the security appliance will boot from, as well as which configuration file it will use at startup.

You can specify up to four local binary image files for use as the startup image, and one image located on a TFTP server for the device to boot from. If you specify an image located on a TFTP server, it must be first in the list. In the event the device cannot reach the TFTP server to load the image from, it will attempt to load the next image file in the list located in Flash.

If you do not specify any boot variable, the first valid image on internal flash will be chosen to boot the system.

Fields

- **Boot Order**—Displays the order in which binary image files will be used to boot.
- **Boot Image Location**—Displays the physical location and path of the boot file.
- **Boot Configuration File Path**—Displays the location of the configuration file.
- **Add**—Lets you add a flash or TFTP boot image entry to be used in the boot process.
- **Edit**—Lets you edit a flash or TFTP boot image entry.
- **Delete**—Deletes the selected flash or TFTP boot image entry.
- **Move Up**—Moves the selected flash or TFTP boot image entry up in the boot order.
- **Move Down**—Moves the selected flash or TFTP boot image entry down in the boot order.
- **Browse Flash**—Lets you specify the location of a boot image or configuration file.

ASDM Image Configuration

- **ASDM Image File Path**—Displays the location of the configuration file the device will use at startup.
- **Browse Flash**—Lets you specify the location of a boot image or configuration file.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Add Boot Image

To add a boot image entry to the boot order list, click **Add** in the Boot Image/Configuration pane.

You can select a Flash or TFTP image to add a boot image to the boot order list.

Either type the path of the image, or click **Browse Flash** to specify the image location. You must type the path of the image location if you are using TFTP.

Fields

- **Flash Image**—Select to add a boot image located in the flash file system.
 - **Path**—Specify the path of the boot image in the flash file system.
- **TFTP Image**—Select to add a boot image located on a TFTP server.
 - **[Path]**—Enter the path on the TFTP server of the boot image file, including the IP address of the server.
- **OK**—Accepts changes and returns to the previous pane.
- **Cancel**—Discards changes and returns to the previous pane.
- **Help**—Provides more information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	•

Device Name/Password

The Device Name/Password pane lets you set the hostname and domain name for the security appliance and set the enable and telnet passwords.

The hostname appears in the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The hostname is also used in system messages.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line; it can be used for a banner.

The security appliance appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the security appliance qualifies the name to “jupiter.example.com.”

The Telnet Password sets the login password. By default, it is “cisco.” Although this area is called Telnet Password, this password applies to Telnet and SSH access. The login password lets you access EXEC mode if you connect to the security appliance using a Telnet or SSH session. (If you configure user authentication for Telnet or SSH access, then each user has their own password, and this login password is not used.)

The enable password lets you access privileged EXEC mode after you log in. Also, this password is used to access ASDM as the default user, which is blank. The default user shows as “enable_15” in the User Accounts pane. (If you configure user authentication for enable access, then each user has their own password, and this enable password is not used; see [About Authentication, page 14-2](#). In addition, you can configure authentication for HTTP/ASDM access.)

Fields

The Hostname and Domain Name area contains the following fields:

- Hostname—Sets the hostname. The default hostname depends on your platform.
- Domain Name—Sets the domain name. The default domain name is default.domain.invalid.

The Enable Password area contains the following fields. In multiple context mode, the Enable Password area only appears in contexts; it does not appear in the system execution space.

- Change the privileged mode password—Lets you change the enable password.
- Old Password—Enter the old password.
- New Password—Enter the new password.
- Confirm New Password—Confirm the new password.

The Telnet Password area contains the following fields. In multiple context mode, the Telnet Password area only appears in contexts; it does not appear in the system execution space.

- Change the password to access the platform console—Lets you change the login password.
- Old Password—Enter the old password.
- New Password—Enter the new password.
- Confirm New Password—Confirm the new password.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

System Software

The System Software pane lets you configure the parameters of security appliances configured as Auto Update clients when this security appliance is acting as an Auto Update server.

As an Auto Update server, you can specify the platform and ASDM images for security appliances configured as Auto Update clients, including image revision numbers and locations, according to the device ID, device family, or device type of the client.

The Auto Update specification provides the infrastructure necessary for remote management applications to download security appliance configurations, software Images, and to perform basic monitoring from a centralized location.

As an Auto Update server, the specification allows the Auto Update server to either push configuration information and send requests for information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time. Communication between the Auto Update server and the security appliance requires a communications path and local CLI configuration on each security appliance.

Fields

The Client Update pane consists of the following fields:

- Enable Client Update—Check to allow the security appliance to update the images used by other security appliances that are configured as Auto Update clients.
- Client Images table—lets you view previously-configured Client Update entries and includes the following columns:
 - Device—Displays a text string corresponding to a device-id of the client.
 - Device Family—Displays the family name of a client, either asa, pix, or a text string.
 - Device Type—Displays the type name of a client.
 - Image Type—Specifies the type of image, either ASDM image or Boot image.
 - Image URL—Specifies the URL for the software component.

- Client Revision—Specifies the revision number(s) of the software component.

Double-clicking any of the rows in the Client Images table opens the Edit Client Update Entry dialog box, in which you can modify the client parameters. These changes are immediately reflected in the table, but you must click Apply to save them to the configuration.

- Live Client Update area—Lets you immediately update Auto Update clients that are currently connected to the security appliance through a tunnel.
 - Tunnel Group—Select “all” to update all Auto Update clients connected over all tunnel groups, or specify a tunnel group for clients that you want to update.
 - Update Now—Click to begin an immediate update.



Note Live Client Update is only available when the security appliance is configured in routed mode.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Client Update

Fields

The Add/Edit Client Update dialog box displays the following fields:

- Device Identification group:
 - Device ID—Enable if the client is configured to identify itself with a unique string, and specify the same string that the client uses. The maximum length is 63 characters.
 - Device Family—Enable if the client is configured to identify itself by device family, and specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.
 - Device Type—Enable if the client is configured to identify itself by device type, and specify the same device type that the client uses. It can be pix-515, pix-515e, pix-525, pix-535, asa5505, asa5510, asa5520, or asa5540. It can also be a text string with a maximum length of 15 characters.
 - Not Specified—Select for clients that do not match the above.
- Image Type—Specifies an image type, either ASDM or boot image. This URL must point to a file appropriate for this client. Maximum length of 255 characters.
- Client Revision—Specifies a text string corresponding to the revision number(s) of the software component. For example: 7.1(0)22.
- Image URL—Specifies the URL for the software component. This URL must point to a file appropriate for this client.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—



CHAPTER 7

Configuring Interfaces in Single Mode

This chapter describes how to configure and enable physical Ethernet interfaces, how to create redundant interface pairs, and how to add subinterfaces. If you have both fiber and copper Ethernet ports (for example, on the 4GE SSM for the ASA 5510 and higher series adaptive security appliance), this chapter describes how to configure the interface media type. For each interface (physical, redundant, or subinterface), you must also configure a name, security level, and IP address (routed mode only).



Note

To configure interfaces for the ASA 5505 adaptive security appliance, see [Chapter 9, “Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance.”](#)

To configure interfaces in multiple context mode, see [Chapter 8, “Configuring Interfaces in Multiple Mode.”](#)

This chapter includes the following sections:

- [Interface Overview, page 7-1](#)
- [Configuring an Interface \(Single Mode\), page 7-5](#)
- [Enabling Same Security Level Communication \(Single Mode\), page 7-8](#)
- [PPPoE IP Address and Route Settings, page 7-9](#)

Interface Overview

This section describes physical interfaces, redundant interfaces, and subinterfaces, and includes the following topics:

- [Physical Interface Overview, page 7-1](#)
- [Redundant Interface Overview, page 7-2](#)
- [VLAN Subinterface and 802.1Q Trunking Overview, page 7-3](#)
- [Default State of Interfaces, page 7-4](#)
- [Default Security Level, page 7-4](#)

Physical Interface Overview

This section describes physical interfaces, and includes the following topics.

- [Default Physical Interface Settings, page 7-2](#)
- [Connector Types, page 7-2](#)
- [Auto-MDI/MDIX Feature, page 7-2](#)

Default Physical Interface Settings

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

Connector Types

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default.

To use the fiber SFP connectors, you must set the media type to SFP. The fiber interface has a fixed speed and does not support duplex, but you can set the interface to negotiate link parameters (the default) or not to negotiate.

Auto-MDI/MDIX Feature

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Redundant Interface Overview

A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to 8 redundant interface pairs.

All subsequent security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.

This section includes overview information about redundant interfaces, and includes the following topics:

- [Redundant Interfaces and Failover Guidelines, page 7-2](#)
- [Redundant Interface MAC Address, page 7-3](#)
- [Physical Interface Guidelines for Use in a Redundant Interface, page 7-3](#)

Redundant Interfaces and Failover Guidelines

Follow these guidelines when adding member interfaces:

- If you want to use a redundant interface for the failover or state link, then you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.

- If you use a redundant interface for the failover or state link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
- You can monitor redundant interfaces for failover; be sure to reference the logical redundant interface name.
- When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.

Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the [“Configuring an Interface \(Single Mode\)” section on page 7-5](#) or the [“Configuring Security Contexts” section on page 10-16](#)). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Physical Interface Guidelines for Use in a Redundant Interface

Follow these guidelines when adding member interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- When you add a physical interface to the redundant interface, the name, IP address, and security level is removed.



Caution

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

- The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters.
- If you shut down the active interface, then the standby interface becomes active.

VLAN Subinterface and 802.1Q Trunking Overview

Subinterfaces let you divide a physical or redundant interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances.

This section includes the following topics:

- [Maximum Subinterfaces, page 7-4](#)
- [Preventing Untagged Packets on the Physical Interface, page 7-4](#)

Maximum Subinterfaces

To determine how many subinterfaces are allowed for your platform, see [Appendix A, “Feature Licenses and Specifications.”](#)

Preventing Untagged Packets on the Physical Interface

If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair. Because the physical or redundant interface must be enabled for the subinterface to pass traffic, ensure that the physical or redundant interface does not pass traffic by not naming it. If you want to let the physical or redundant interface pass untagged packets, you can configure the name command as usual.

Default State of Interfaces

Interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the security appliance sets the security level to 100.

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the [“Enabling Same Security Level Communication \(Single Mode\)” section on page 7-8](#) for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

If you enable communication between same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

- **Filtering**—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.

- **NAT control**—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

If you enable communication between same security interfaces, you can configure **established** commands for both directions.

Configuring an Interface (Single Mode)

To configure an interface, perform the following steps. For overview information, see the [“Interface Overview” section on page 7-1](#).



Note

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See [Chapter 15, “High Availability,”](#) to configure the failover and state links. You can, however, set physical interface properties such as the speed and duplex using this procedure.

Step 1

Go to the Configuration > Device Setup > Interfaces pane.

By default, all physical interfaces are listed. You can edit a physical interface, or you can add a subinterface or redundant interface.

- To edit a physical interface or any other existing interface, choose the interface row, and click **Edit**.
The Edit Interface dialog box appears with the General tab selected.
- To add and configure a subinterface, perform the following steps:
 - a. Click **Add > Interface**.
The Add Interface dialog box appears with the General tab selected.
 - b. From the Hardware Port drop-down list, choose the physical interface to which you want to add the subinterface.
 - c. In the VLAN ID field, enter the VLAN ID between 1 and 4095.
Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.
 - d. In the Subinterface ID field, enter the subinterface ID as an integer between 1 and 4294967293.
The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.
 - e. Continue configuring the interface by following [Step 2](#).
- To add and configure a redundant interface, perform the following steps:

- a. Click **Add > Redundant Interface**.

The Add Redundant Interface dialog box appears with the General tab selected.

- b. In the Redundant ID field, enter an integer between 1 and 8.
- c. From the Primary Interface drop-down list, choose the physical interface you want to be primary.
Be sure to pick an interface that does not have a subinterface and that has not already been allocated to a context.
- d. From the Secondary Interface drop-down list, choose the physical interface you want to be secondary.
- e. Continue configuring the interface by following [Step 2](#).

Step 2 In the Interface Name field, enter a name up to 48 characters in length.

Step 3 In the Security level field, enter a level between 0 (lowest) and 100 (highest).

See the [“Default Security Level”](#) section on page 7-4 for more information.

Step 4 (Optional) To set this interface as a management-only interface, check **Dedicate this interface to management-only**.

Through traffic is not accepted on a management-only interface.

Step 5 If the interface is not already enabled, check **Enable Interface**.

Step 6 To set the IP address, follow these guidelines:

In routed firewall mode, set the IP address for all interfaces. In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole security appliance or context. The exception is for the Management 0/0 or 0/1 management-only interface, which does not pass through traffic. To set the transparent firewall mode whole security appliance or context management IP address, see the [Management IP Address](#) pane. To set the IP address of the Management interface or subinterface, use this procedure.

For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported. Set the standby IP addresses on the Configuration > Device Management > High Availability > Failover > Interfaces tab.

Use one of the following options to set the IP address:

- To set the IP address manually, click **Use Static IP** and enter the IP address and mask.
- To obtain an IP address from a DHCP server, click **Obtain Address via DHCP**.
 - a. (Optional) To obtain the default route from the DHCP server, check **Obtain Default Route Using DHCP**.
 - b. (Optional) To assign an administrative distance to the learned route, enter a value between 1 and 255 in the DHCP Learned Route Metric field. If this field is left blank, the administrative distance for the learned routes is 1.
 - c. (Optional) To renew the lease, click **Renew DHCP Lease**.
 - d. (Optional) To enable tracking for DHCP-learned routes, check **Enable Tracking for DHCP Learned Routes**. Set the following values:

Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.

Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.

**Note**

Route tracking is only available in single, routed mode.

SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.

Monitor Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.

- To obtain an IP address using PPPoE, check **Use PPPoE**.
 - a. In the Group Name field, specify a group name.
 - b. In the PPPoE Username field, specify the username provided by your ISP.
 - c. In the PPPoE Password field, specify the password provided by your ISP.
 - d. In the Confirm Password field, retype the password.
 - e. For PPP authentication, click either PAP, CHAP, or MSCHAP.

PAP passes cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

- f. (Optional) To store the username and password in Flash memory, check **Store Username and Password in Local Flash**.

The security appliance stores the username and password in a special location of NVRAM. If an Auto Update Server sends a **clear configure** command to the security appliance, and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

- g. (Optional) To display the PPPoE IP Address and Route Settings dialog box where you can choose addressing and tracking options, click **IP Address and Route Settings**. See the [“PPPoE IP Address and Route Settings”](#) section on page 7-9 for more information.

Step 7 (Optional) In the Description field, enter a description for this interface.

The description can be up to 240 characters on a single line, without carriage returns. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

Step 8 (Optional) To set the media type, duplex, and speed, click the **Configure Hardware Properties** button.

- a. If you have an ASA 5550 adaptive security appliance or a 4GE SSM, you can choose either **RJ-45** or **SFP** from the Media Type drop-down list.

RJ-45 is the default.

- b. To set the duplex for RJ-45 interfaces, choose Full, Half, or Auto, depending on the interface type, from the Duplex drop-down list.
- c. To set the speed, choose a value from the Speed drop-down list.

The speeds available depend on the interface type. For fiber interfaces, you can set the speed to Negotiate or Nonnegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonnegotiate does not negotiate link

parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

d. Click **OK** to accept the Hardware Properties changes.

Step 9 (Optional) To set the MTU or to enable jumbo frame support (ASA 5580 only), click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.

The default is 1500 bytes. For the ASA 5580, if you enter a value for any interface that is greater than 1500, then you enable jumbo frame support automatically for all interfaces. If you set the MTU for all interfaces back to a value under 1500, then jumbo frame support is disabled.

**Note**

Enabling or disabling jumbo frame support requires you to reboot the security appliance.

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. Jumbo frames require extra memory to process, and assigning more memory for jumbo frames might limit the the maximum use of other features, such as access lists.

Step 10 (Optional) To manually assign a MAC address to this interface, on the Advanced tab enter a MAC address in the Active Mac Address field in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If you use failover, enter the standby MAC address in the Standby Mac Address field. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this field, then it is used regardless of the member interface MAC addresses.

You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

Step 11 Click **OK**.

Enabling Same Security Level Communication (Single Mode)

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same-security interfaces lets you configure more than 101 communicating interfaces. If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).

**Note**

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

You can also enable communication between hosts connected to the same interface.

- To enable interfaces on the same security level to communicate with each other, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.
- To enable communication between hosts connected to the same interface, check **Enable traffic between two or more hosts connected to the same interface**.

PPPoE IP Address and Route Settings

The PPPoE IP Address and Route Settings dialog lets you choose addressing and tracking options for PPPoE connections.

See the [“Configuring an Interface \(Single Mode\)” section on page 7-5](#) for more information about using PPPoE for an interface.

Fields

- IP Address area—Lets you choose between Obtaining an IP address using PPP or specifying an IP address, and contains the following fields:
 - Obtain IP Address using PPP—Select to enable the security appliance to use PPP to get an IP address.
 - Specify an IP Address—Specify an IP address and mask for the security appliance to use instead of negotiating with the PPPoE server to assign an address dynamically.
- Route Settings Area—Lets you configure route and tracking settings and contains the following fields:
 - Obtain default route using PPPoE—Sets the default routes when the PPPoE client has not yet established a connection. When using this option, you cannot have a statically defined route in the configuration.

PPPoE learned route metric—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.

- Enable tracking—Check this checkbox to enable route tracking for PPPoE-learned routes.



Note Route tracking is only available in single, routed mode.

- Primary Track—Select this option to configure the primary PPPoE route tracking.
- Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.
- Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.
- SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.

- Monitor Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.
- Secondary Track—Select this option to configure the secondary PPPoE route tracking.

Secondary Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.



CHAPTER 8

Configuring Interfaces in Multiple Mode

This chapter describes how to configure and enable physical Ethernet interfaces, how to create redundant interface pairs, and how to add subinterfaces in the system configuration. If you have both fiber and copper Ethernet ports (for example, on the 4GE SSM for the ASA 5510 and higher series adaptive security appliance), this chapter describes how to configure the interface media type.

For each interface assigned to a context (physical, redundant, or subinterface), this chapter tells how to configure a name, security level, and IP address (routed firewall mode only).



Note

To configure interfaces in single context mode, see [Chapter 7, “Configuring Interfaces in Single Mode.”](#)

This chapter includes the following sections:

- [Configuring Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-1
- [Allocating Interfaces to Contexts](#), page 8-7
- [Configuring Interface Parameters within each Context \(Multiple Mode\)](#), page 8-7

Configuring Interfaces in the System Configuration (Multiple Mode)

In multiple context mode, you configure physical interface parameters and add redundant interfaces and subinterfaces in the system execution space.

This chapter includes the following sections:

- [Configuring Physical Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-2
- [Configuring Redundant Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-3
- [Configuring VLAN Subinterfaces and 802.1Q Trunking in the System Configuration \(Multiple Mode\)](#), page 8-5
- [Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration \(Multiple Mode\)](#), page 8-7

**Note**

If you use failover, you need to assign a dedicated interface as the failover link and an optional interface for Stateful Failover on the [Failover: Setup](#) tab. (You can use the same interface for failover and state traffic, but we recommend separate interfaces). You can use a physical interface, subinterface, or redundant interface for the failover and state links, as long as they are not assigned to a context. To use a subinterface, do not assign the physical interface to a context.

Configuring Physical Interfaces in the System Configuration (Multiple Mode)

This section describes how to configure settings for physical interfaces, and includes the following topics:

- [Physical Interface Overview, page 8-2](#)
- [Configuring and Enabling Physical Interfaces in the System Configuration \(Multiple Mode\), page 8-3](#)

Physical Interface Overview

This section describes physical interfaces, and includes the following topics:

- [Default State of Physical Interfaces, page 8-2](#)
- [Connector Types, page 8-2](#)
- [Auto-MDI/MDIX Feature, page 8-2](#)

Default State of Physical Interfaces

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through it (either alone or as part of a redundant interface pair), or through a subinterface. For multiple context mode, if you allocate an interface (physical, redundant, or subinterface) to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must first enable the physical interface in the system configuration according to this procedure.

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

Connector Types

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default.

To use the fiber SFP connectors, you must set the media type to SFP. The fiber interface has a fixed speed and does not support duplex, but you can set the interface to negotiate link parameters (the default) or not to negotiate.

Auto-MDI/MDIX Feature

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Configuring and Enabling Physical Interfaces in the System Configuration (Multiple Mode)

To configure and enable a physical interface, perform the following steps:

-
- Step 1** In the Configuration > Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Interfaces pane, click a physical interface that you want to configure, and click **Edit**.
- Step 3** To enable the interface, check the **Enable Interface** check box.
- Step 4** To add a description, enter text in the Description field.
- Step 5** (Optional) To set the media type, duplex, and speed, click the **Configure Hardware Properties** button.
- If you have an ASA 5550 adaptive security appliance or a 4GE SSM, you can choose either **RJ-45** or **SFP** from the Media Type drop-down list.
RJ-45 is the default.
 - To set the duplex for RJ-45 interfaces, choose Full, Half, or Auto, depending on the interface type, from the Duplex drop-down list.
 - To set the speed, choose a value from the Speed drop-down list.
The speeds available depend on the interface type. For fiber interfaces, you can set the speed to Negotiate or Nonegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonegotiate does not negotiate link parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.
 - Click **OK** to accept the Hardware Properties changes.
- Step 6** Click **OK** to accept the Interface changes.
-

Configuring Redundant Interfaces in the System Configuration (Multiple Mode)

A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to 8 redundant interface pairs.

All subsequent security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.

This section describes how to configure redundant interfaces, and includes the following topics:

- [Redundant Interface Overview, page 8-4](#)
- [Adding a Redundant Interface in the System Configuration \(Multiple Mode\), page 8-5](#)

Redundant Interface Overview

This section includes overview information about redundant interfaces, and includes the following topics:

- [Default State of Redundant Interfaces, page 8-4](#)
- [Redundant Interfaces and Failover Guidelines, page 8-4](#)
- [Redundant Interface MAC Address, page 8-4](#)
- [Physical Interface Guidelines for Use in a Redundant Interface, page 8-4](#)

Default State of Redundant Interfaces

When you add a redundant interface, it is enabled by default. However, the member interfaces must also be enabled to pass traffic.

Redundant Interfaces and Failover Guidelines

Follow these guidelines when adding member interfaces:

- If you want to use a redundant interface for the failover or state link, then you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.
- If you use a redundant interface for the failover or state link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
- You can monitor redundant interfaces for failover; be sure to reference the logical redundant interface name.
- When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.

Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the [“Configuring Interface Parameters in each Context \(Multiple Mode\)” section on page 8-9](#) or the [“Configuring Security Contexts” section on page 10-16](#)). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Physical Interface Guidelines for Use in a Redundant Interface

Follow these guidelines when adding member interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- When you add a physical interface to the redundant interface, the name, IP address, and security level is removed.

**Caution**

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

- If you shut down the active interface, then the standby interface becomes active.

Adding a Redundant Interface in the System Configuration (Multiple Mode)

You can configure up to 8 redundant interface pairs. To configure a redundant interface, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click System under the active device IP address. |
| Step 2 | On the Context Management > Interfaces pane, click Add > Redundant Interface . |
| Step 3 | In the Redundant ID field, enter an integer between 1 and 8. |
| Step 4 | From the Primary Interface drop-down list, choose the physical interface you want to be primary.
Be sure to pick an interface that does not have a subinterface and that has not already been allocated to a context. |
| Step 5 | From the Secondary Interface drop-down list, choose the physical interface you want to be secondary. |
| Step 6 | If the interface is not already enabled, check Enable Interface .
The interface is enabled by default. To disable it, uncheck the box. |
| Step 7 | To add a description, enter text in the Description field.
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link. |
| Step 8 | Click OK . |
-

Configuring VLAN Subinterfaces and 802.1Q Trunking in the System Configuration (Multiple Mode)

This section describes how to configure a subinterface, and includes the following topics:

- [Subinterface Overview, page 8-5](#)
- [Adding a Subinterface in the System Configuration \(Multiple Mode\), page 8-6](#)

Subinterface Overview

Subinterfaces let you divide a physical or redundant interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

This section includes the following topics:

- [Default State of Subinterfaces, page 8-6](#)

- [Maximum Subinterfaces, page 8-6](#)

Default State of Subinterfaces

When you add a subinterface, it is enabled by default. However, the physical or redundant interface must also be enabled to pass traffic (see the [“Configuring Physical Interfaces in the System Configuration \(Multiple Mode\)”](#) section on page 8-2 to enable physical interfaces. See the [“Configuring Redundant Interfaces in the System Configuration \(Multiple Mode\)”](#) section on page 8-3 to enable redundant interfaces).

Maximum Subinterfaces

To determine how many subinterfaces are allowed for your platform, see [Appendix A, “Feature Licenses and Specifications.”](#)

Adding a Subinterface in the System Configuration (Multiple Mode)

To add a subinterface and assign a VLAN to it, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click System under the active device IP address. |
| Step 2 | On the Context Management > Interfaces pane, click Add > Interface . |
| Step 3 | From the Hardware Port drop-down list, choose the physical interface to which you want to add the subinterface. |
| Step 4 | If the interface is not already enabled, check Enable Interface .
The interface is enabled by default. To disable it, uncheck the box. |
| Step 5 | In the VLAN ID field, enter the VLAN ID between 1 and 4095.
Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration. |
| Step 6 | In the Subinterface ID field, enter the subinterface ID as an integer between 1 and 4294967293.
The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it. |
| Step 7 | (Optional) In the Description field, enter a description for this interface.
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link. |
| Step 8 | Click OK . |
-

Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration (Multiple Mode)

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all Gigabit and 10-Gigabit interfaces on interface adapters by increasing the amount of memory to process Ethernet frames. Jumbo frames are not supported on the embedded Management ports. Enabling jumbo frame support might limit the maximum use of other features, such as access lists.

To enable jumbo frame support, go to the Configuration > Interfaces pane, and click the **Enable jumbo frame support** check box.

**Note**

Changes in this setting require you to reboot the security appliance.

**Note**

Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9000. See the [“Configuring Interface Parameters in each Context \(Multiple Mode\)”](#) section on page 8-9 to configure the MTU within each context.

Allocating Interfaces to Contexts

To allocate interfaces to contexts, see the [“Configuring Security Contexts”](#) section on page 10-16.

Configuring Interface Parameters within each Context (Multiple Mode)

Within each context, you configure the name, security level, and IP address of each interface. You can also enable same security level communication. This section includes the following topics:

- [Interface Parameters Overview, page 8-7](#)
- [Configuring Interface Parameters in each Context \(Multiple Mode\), page 8-9](#)
- [Enabling Same Security Level Communication \(Multiple Mode\), page 8-10](#)

Interface Parameters Overview

This section describes interface parameters and includes the following topics:

- [Default State of Interfaces, page 8-8](#)
- [Default Security Level, page 8-8](#)

Default State of Interfaces

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the security appliance sets the security level to 100.



Note

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the [“Enabling Same Security Level Communication \(Multiple Mode\)” section on page 8-10](#) for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.
For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.
- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).
For same security interfaces, you can filter traffic in either direction.
- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for some security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For some security interfaces, you can configure **established** commands for both directions.

Configuring Interface Parameters in each Context (Multiple Mode)

To add or edit an interface, perform the following steps.

-
- Step 1** In the Configuration > Device List pane, double-click the context name under the active device *IP address* > Contexts.
- Step 2** On the Device Setup > Interfaces pane, click an interface that you want to configure, and click **Edit**. The Add/Edit Interface dialog box appears with the General tab selected.
- Step 3** In the Interface Name field, enter a name up to 48 characters in length.
- Step 4** In the Security level field, enter a level between 0 (lowest) and 100 (highest). See the [“Default Security Level”](#) section on page 8-8 for more information.
- Step 5** (Optional) To set this interface as a management-only interface, check **Dedicate this interface to management-only**.
Through traffic is not accepted on a management-only interface.
- Step 6** If the interface is not already enabled, check **Enable Interface**.
The interface is enabled by default. To disable it, uncheck the box.
- Step 7** To set the IP address, use one of the following options.
In routed firewall mode, set the IP address for all interfaces. In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole security appliance or context. The exception is for the Management 0/0 management-only interface, which does not pass through traffic. To set the transparent firewall mode whole security appliance or context management IP address, see the [Management IP Address](#) pane. To set the IP address of the Management 0/0 interface or subinterface, use this procedure.
For use with failover, you must set the IP address and standby address manually; DHCP is not supported. Set the standby IP addresses on the Configuration > Device Management > High Availability > Failover > Interfaces tab.
- To set the IP address manually, click **Use Static IP** and enter the IP address and mask.
 - To obtain an IP address from a DHCP server, click **Obtain Address via DHCP**.
 - a. (Optional) To obtain the default route from the DHCP server, check **Obtain Default Route Using DHCP**.
 - b. (Optional) To renew the lease, click **Renew DHCP Lease**.
- Step 8** (Optional) In the Description field, enter a description for this interface.

The description can be up to 240 characters on a single line, without carriage returns. The system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

- Step 9** (Optional) To set the MTU, click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.

The default is 1500 bytes. For the ASA 5580, if you set the value above 1500 bytes, be sure to enable jumbo frame support in the system configuration (see the [“Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration \(Multiple Mode\)”](#) section on page 8-7).

- Step 10** (Optional) To manually assign a MAC address to this interface, on the Advanced tab enter a MAC address in the Active Mac Address field in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If you use failover, enter the standby MAC address in the Standby Mac Address field. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this field, then it is used regardless of the member interface MAC addresses.

If you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the [“How the Security Appliance Classifies Packets”](#) section on page 10-2 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See the [“Automatically Assigning MAC Addresses”](#) section on page 10-17 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this option to override the generated address.

For interfaces that are not shared, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

- Step 11** Click **OK**.

Enabling Same Security Level Communication (Multiple Mode)

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same-security interfaces lets you configure more than 101 communicating interfaces. If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).



Note

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

You can also enable communication between hosts connected to the same interface.

- To enable interfaces on the same security level to communicate with each other, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.
- To enable communication between hosts connected to the same interface, check **Enable traffic between two or more hosts connected to the same interface**.



CHAPTER 9

Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance

This chapter describes how to configure the switch ports and VLAN interfaces of the ASA 5505 adaptive security appliance.



Note

To configure interfaces of other models, see [Chapter 7, “Configuring Interfaces in Single Mode.”](#)

This chapter includes the following sections:

- [Interface Overview, page 9-1](#)
- [Configuring VLAN Interfaces, page 9-5](#)
- [Configuring Switch Ports, page 9-11](#)

Interface Overview

This section describes the ports and interfaces of the ASA 5505 adaptive security appliance, and includes the following topics:

- [Understanding ASA 5505 Ports and Interfaces, page 9-2](#)
- [Maximum Active VLAN Interfaces for Your License, page 9-2](#)
- [Default Interface Configuration, page 9-4](#)
- [VLAN MAC Addresses, page 9-4](#)
- [Power Over Ethernet, page 9-4](#)
- [Monitoring Traffic Using SPAN, page 9-4](#)
- [Security Level Overview, page 9-5](#)

Understanding ASA 5505 Ports and Interfaces

The ASA 5505 adaptive security appliance supports a built-in switch. There are two kinds of ports and interfaces that you need to configure:

- Physical switch ports—The adaptive security appliance has eight Fast Ethernet switch ports that forward traffic at Layer 2, using the switching function in hardware. Two of these ports are PoE ports. See the [“For same security interfaces, you can configure established commands for both directions.” section on page 9-5](#) for more information. You can connect these interfaces directly to user equipment such as PCs, IP phones, or a DSL modem. Or you can connect to another switch.
- Logical VLAN interfaces—In routed mode, these interfaces forward traffic between VLAN networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces forward traffic between the VLANs on the same network at Layer 2, using the configured security policy to apply firewall services. See the [“Maximum Active VLAN Interfaces for Your License”](#) section for more information about the maximum VLAN interfaces. VLAN interfaces let you divide your equipment into separate VLANs, for example, home, business, and Internet VLANs.

To segregate the switch ports into separate VLANs, you assign each switch port to a VLAN interface. Switch ports on the same VLAN can communicate with each other using hardware switching. But when a switch port on VLAN 1 wants to communicate with a switch port on VLAN 2, then the adaptive security appliance applies the security policy to the traffic and routes or bridges between the two VLANs.

**Note**

Subinterfaces are not available for the ASA 5505 adaptive security appliance.

Maximum Active VLAN Interfaces for Your License

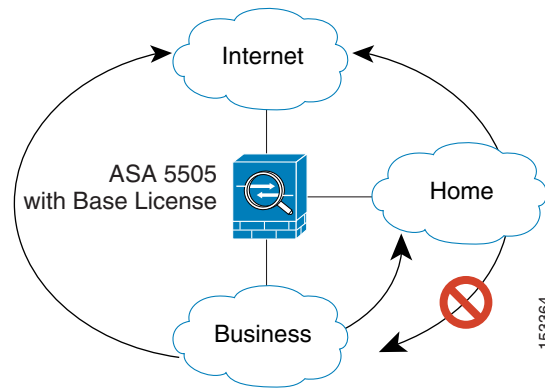
In transparent firewall mode, you can configure two active VLANs in the Base license and three active VLANs in the Security Plus license, one of which must be for failover.

In routed mode, you can configure up to three active VLANs with the Base license, and up to 20 active VLANs with the Security Plus license.

An active VLAN is a VLAN with a **nameif** command configured.

With the Base license, the third VLAN can only be configured to initiate traffic to one other VLAN. See [Figure 9-1](#) for an example network where the Home VLAN can communicate with the Internet, but cannot initiate contact with Business.

Figure 9-1 *ASA 5505 Adaptive Security Appliance with Base License*



With the Security Plus license, you can configure 20 VLAN interfaces. You can configure trunk ports to accommodate multiple VLANs per port.

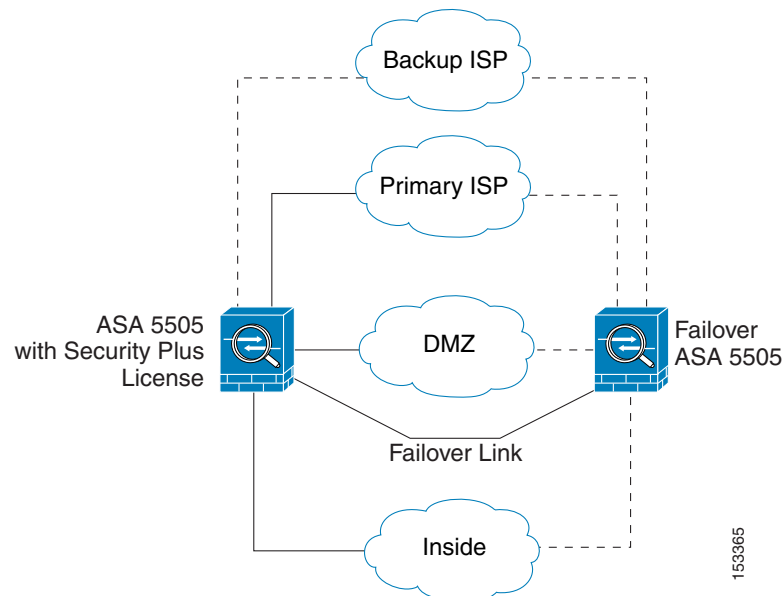


Note

The ASA 5505 adaptive security appliance supports Active/Standby failover, but not Stateful failover.

See [Figure 9-2](#) for an example network.

Figure 9-2 *ASA 5505 Adaptive Security Appliance with Security Plus License*



Default Interface Configuration

If your adaptive security appliance includes the default factory configuration, your interfaces are configured as follows:

- The outside interface (security level 0) is VLAN 2.
Ethernet0/0 is assigned to VLAN 2 and is enabled.
The VLAN 2 IP address is obtained from the DHCP server.
- The inside interface (security level 100) is VLAN 1
Ethernet 0/1 through Ethernet 0/7 are assigned to VLAN 1 and is enabled.
VLAN 1 has IP address 192.168.1.1.

Restore the default factory configuration using the **configure factory-default** command.

Use the procedures in this chapter to modify the default configuration, for example, to add VLAN interfaces.

If you do not have a factory default configuration, all switch ports are in VLAN 1, but no other parameters are configured.

VLAN MAC Addresses

In routed firewall mode, all VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses.

In transparent firewall mode, each VLAN has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses.

Power Over Ethernet

Ethernet 0/6 and Ethernet 0/7 support PoE for devices such as IP phones or wireless access points. If you install a non-PoE device or do not connect to these switch ports, the adaptive security appliance does not supply power to the switch ports.

If you shut down the switch port from the [Edit Switch Port](#) dialog box, you disable power to the device. Power is restored when you enter reenable it.

To view the status of PoE switch ports, including the type of device connected (Cisco or IEEE 802.3af), use the **show power inline** command.

Monitoring Traffic Using SPAN

If you want to monitor traffic that enters or exits one or more switch ports, you can enable SPAN, also known as switch port monitoring. The port for which you enable SPAN (called the destination port) receives a copy of every packet transmitted or received on a specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor all traffic; without SPAN, you would have to attach a sniffer to every port you want to monitor. You can only enable SPAN for one destination port.

You can only enable SPAN monitoring using the Command Line Interface tool by entering the **switchport monitor** command. See the **switchport monitor** command in the *Cisco Security Appliance Command Reference* for more information.

Security Level Overview

Each VLAN interface must have a security level in the range 0 to 100 (from lowest to highest). For example, you should assign your most secure network, such as the inside business network, to level 100. The outside network connected to the Internet can be level 0. Other networks, such as a home network can be in between. You can assign interfaces to the same security level.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the adaptive security appliance.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For same security interfaces, you can configure **established** commands for both directions.

Configuring VLAN Interfaces

For information about how many VLANs you can configure, see the [“Maximum Active VLAN Interfaces for Your License” section on page 9-2](#).



Note

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover communications. See [Chapter 15, “High Availability,”](#) to configure the failover link.

If you enabled Easy VPN, you cannot add or delete VLAN interfaces, nor can you edit the security level or interface name. We suggest that you finalize your interface configuration before you enable Easy VPN.

This section includes the following topics:

- [Interfaces > Interfaces, page 9-6](#)
- [Add/Edit Interface > General, page 9-8](#)
- [Add/Edit Interface > Advanced, page 9-10](#)

Interfaces > Interfaces

The Interfaces tab displays configured VLAN interfaces. You can add or delete VLAN interfaces, and also enable communication between interfaces on the same security level or enable traffic to enter and exit the same interface.

Transparent firewall mode allows only two interfaces to pass through traffic.

Fields

- Name—Displays the interface name.
- Switch Ports—Shows the switch ports assigned to this VLAN interface.
- Enabled—Indicates if the interface is enabled, Yes or No.
- Security Level—Displays the interface security level between 0 and 100. By default, the security level is 0.
- IP Address—Displays the IP address, or in transparent mode, the word “native.” Transparent mode interfaces do not use IP addresses. To set the IP address for the context or the security appliance, see the [Management IP Address](#) pane.
- Subnet Mask—For routed mode only. Displays the subnet mask.
- Restrict Traffic Flow—Shows if this interface is restricted from initiating contact to another VLAN.

With the Base license, you can only configure a third VLAN if you use this option to limit it.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the Restrict Traffic Flow option on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

If you already have two VLAN interfaces configured with a name, be sure to enable the Restrict Traffic Flow option before you name the third interface; the adaptive security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance.



Note

If you upgrade to the Security Plus license, you can remove this option and achieve full functionality for this interface. If you leave this option enabled, this interface continues to be limited even after upgrading.

- Backup Interface—Shows the backup ISP interface for this interface. If this interface fails, the backup interface takes over.

The backup interface does not pass through traffic unless the default route through the primary interface fails. This option is useful for Easy VPN; when the backup interface becomes the primary, the security appliance moves the VPN rules to the new primary interface.

To ensure that traffic can pass over the backup interface in case the primary fails, be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. To configure dual ISP support, see the [“Static Route Tracking” section on page 11-41](#).

- **VLAN**—Shows the VLAN ID for this interface.
- **Management Only**—Indicates if the interface allows traffic to the security appliance or for management purposes only.
- **MTU**—Displays the MTU. By default, the MTU is 1500.
- **Active MAC Address**—Shows the active MAC address, if you assigned one manually on the [Add/Edit Interface > Advanced](#) tab.
- **Standby MAC Address**—Shows the standby MAC address (for failover), if you assigned one manually.
- **Description**—Displays a description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description.
- **Add**—Adds an interface. If you enabled Easy VPN, you cannot add VLAN interfaces.
- **Edit**—Edits the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot edit the interface in this pane. If you enabled Easy VPN, you cannot edit the security level or interface name.
- **Delete**—Deletes the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot delete the interface in this pane. If you enabled Easy VPN, you cannot delete VLAN interfaces.
- **Enable traffic between two or more interfaces which are configured with same security levels**—Enables communication between interfaces on the same security level. If you enable same security interface communication, you can still configure interfaces at different security levels as usual.
- **Enable traffic between two or more hosts connected to the same interface**—Enables traffic to enter and exit the same interface.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Interface > General

The Add/Edit Interface > General tab lets you add or edit a VLAN interface.

If you intend to use an interface for failover, do not configure the interface in this dialog box; instead, use the [Failover: Setup](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored.

If you enabled Easy VPN, you cannot edit the security level or interface name. We suggest that you finalize your interface configuration before you enable Easy VPN.

After you assign the interface as the failover link or state link, you cannot edit or delete the interface from the Interfaces pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

Fields

- Switch Ports—Assigns switch ports to this VLAN interface.
 - Available Switch Ports—Lists all switch ports, even if they are currently assigned to a different interface.
 - Selected Switch Ports—Lists the switch ports assigned to this interface.
 - Add—Adds a selected switch port to the interface. You see the following message:
“switchport is associated with name interface. Adding it to this interface, will remove it from name interface. Do you want to continue?”
 Click **OK** to add the switch port.
 You will always see this message when adding a switch port to an interface; switch ports are assigned to the VLAN 1 interface by default even when you do not have any configuration.
 - Remove—Removes a switch port from an interface. Because the default VLAN interface for switch ports is VLAN 1, removing a switch port from an interface essentially just reassigns that switch port to VLAN 1.
- Enable Interface—Enables this interface to pass traffic. In addition to this setting, you need to set an IP address (for routed mode) and a name before traffic can pass according to your security policy.
- Dedicate this interface to management only—Sets the interface to accept traffic to the security appliance only, and not through traffic. You cannot set a primary or backup ISP interface to be management only.
- Interface Name—Sets an interface name up to 48 characters in length.
- Security Level—Sets the security level between 0 (lowest) and 100 (highest). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.
- IP Address—For routed mode only, sets the IP address.
 - Use Static IP—Manually sets the IP address.
 IP address—Sets the IP address.
 Subnet Mask—Sets the subnet mask.
 - Obtain Address via DHCP—Dynamically sets the IP address using DHCP.
 Obtain Default Route Using DHCP—Obtains a default route from the DHCP server so that you do not need to configure a default static route.
 Renew DHCP Lease—Renews the DHCP lease.

Retry Count—Sets the number of times between 4 and 16 that the security appliance resends a DHCP request if it does not receive a reply after the first attempt. The total number of attempts is the retry count plus the first attempt. For example, if you set the retry count to 4, the security appliance sends up to 5 DHCP requests.

DHCP Learned Route Metric—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.

Enable tracking—Check this checkbox to enable route tracking for DHCP-learned routes.



Note Route tracking is only available in single, routed mode.

Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.

Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.

SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.

Monitor Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.

- Use PPPoE—Dynamically sets the IP address using PPPoE.

Group Name—Specify a group name.

PPPoE Username—Specify the username provided by your ISP.

PPPoE Password—Specify the password provided by your ISP.

Confirm Password—Specify the password provided by your ISP.

PPP Authentication—Select either PAP, CHAP, or MSCHAP. PAP passes cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

Store Username and Password in Local Flash—Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

IP Address and Route Settings—displays the PPPoE IP Address and Route Settings dialog where you can choose addressing and tracking options. See the [“PPPoE IP Address and Route Settings” section on page 7-9](#).

- **Description**—Sets an optional description up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Interface > Advanced

The Add/Edit Interface > Advanced tab lets you set the MTU, VLAN ID, MAC addresses, and other options.

Fields

- **MTU**—Sets the MTU from 300 to 65,535 bytes. The default is 1500 bytes. For multiple context mode, set the MTU in the context configuration.
- **VLAN ID**—Sets the VLAN ID for this interface between 1 and 4090. If you do not want to assign the VLAN ID, ASDM assigns one for you randomly.
- **Mac Address Cloning**—Manually assigns MAC addresses.

By default in routed mode, all VLANs use the same MAC address. In transparent mode, the VLANs use unique MAC addresses. You might want to set unique VLANs or change the generated VLANs if your switch requires it, or for access control purposes.

- **Active Mac Address**—Assigns a MAC address to the interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.
- **Standby Mac Address**—For use with failover, set the Standby Mac Address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.
- **Block Traffic**—Restrict this VLAN interface from initiating contact to another VLAN.

With the Base license, you can only configure a third VLAN if you use this option to limit it.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the Restrict Traffic Flow option on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

If you already have two VLAN interfaces configured with a name, be sure to enable the Restrict Traffic Flow option before you name the third interface; the adaptive security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance and will not allow you to configure one.



Note

If you upgrade to the Security Plus license, you can remove this option and achieve full functionality for this interface. If you leave this option enabled, this interface continues to be limited even after upgrading.

- Block Traffic from this Interface to—Choose a VLAN ID in the list.
- Select Backup Interface—Shows the backup ISP interface for this interface. If this interface fails, the backup interface takes over. The backup interface does not pass through traffic unless the default route through the primary interface fails. This option is useful for Easy VPN; when the backup interface becomes the primary, the security appliance moves the VPN rules to the new primary interface.

To ensure that traffic can pass over the backup interface in case the primary fails, be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. To configure dual ISP support, see the [“Static Route Tracking” section on page 11-41](#).

- Backup Interface—Choose a VLAN ID in the list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Configuring Switch Ports

This section describes how to configure switch ports, and includes the following topics:

- [Interfaces > Switch Ports, page 9-11](#)
- [Edit Switch Port, page 9-12](#)



Caution

The ASA 5505 adaptive security appliance does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the adaptive security appliance does not end up in a network loop.

Interfaces > Switch Ports

The Switch Ports tab displays the switch port parameters.

Fields

- Switch Port—Lists the switch ports in the security appliance.
- Enabled—Shows if the switch port is enabled, Yes or No.
- Associated VLANs—Lists the VLAN interfaces to which the switch port is assigned. A trunk switch port can be associated with multiple VLANs.
- Associated Interface Names—Lists the VLAN interface names.

- **Mode**—The mode, Access or Trunk. Access ports can be assigned to one VLAN. Trunk ports can carry multiple VLANs using 802.1Q tagging. Trunk mode is available only with the Security Plus license.
- **Protected**—Shows if this switch port is protected, Yes or No. This option prevents the switch port from communicating with other protected switch ports on the same VLAN. You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the Protected option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
- **Edit**—Edits the switch port.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Edit Switch Port

The Edit Switch Port dialog box lets you configure the mode, assign a switch port to a VLAN, and set the Protected option.

Fields

- **Switch Port**—*Display only*. Shows the selected switch port ID.
- **Enable Switch Port**—Enables this switch port.
- **Mode and VLAN IDs**—Sets the mode and the assigned VLANs.
 - **Access VLAN ID**—Sets the mode to access mode. Enter the VLAN ID to which you want to assign this switch port. By default, the VLAN ID is derived from the VLAN interface configuration in [Interfaces > Interfaces](#). You can change the VLAN assignment in this dialog box. Be sure to apply the change to update the [Interfaces > Interfaces](#) tab with the new information. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN from the [Interfaces > Interfaces](#) tab and specify the switch port in the [Add/Edit Interface > General](#) tab rather than specifying it in this dialog box; in either case, you need to add the VLAN on the [Interfaces > Interfaces](#) tab and assign the switch port to it.
 - **Trunk VLAN IDs**—Sets the mode to trunk mode using 802.1Q tagging. Trunk mode is available only with the Security Plus license. Enter the VLAN IDs to which you want to assign this switch port, separated by commas. Trunk ports do not support untagged packets; there is no native VLAN support, and the adaptive security appliance drops all packets that do not contain a tag specified in this command. If the VLANs are already in your configuration, after you apply the change, the [Interfaces > Interfaces](#) tab shows this switch port added to each VLAN. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN from the

[Interfaces > Interfaces](#) tab and specify the switch port in the [Add/Edit Interface > General](#) tab rather than specifying it in this dialog box; in either case, you need to add the VLAN on the [Interfaces > Interfaces](#) tab and assign the switch port to it.

- **Isolated**—This option prevents the switch port from communicating with other protected switch ports on the same VLAN. You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the Protected option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
 - **Isolated**—Sets this switch port as a protected port.
- **Duplex**—Lists the duplex options for the interface, including Full, Half, or Auto. The Auto setting is the default. If you set the duplex to anything other than Auto on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.
- **Speed**—The Auto setting is the default. If you set the speed to anything other than Auto on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power. The default Auto setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to Auto to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—



CHAPTER 10

Configuring Security Contexts

This chapter describes how to use security contexts and enable multiple context mode. This chapter includes the following sections:

- [Security Context Overview, page 10-1](#)
- [Enabling or Disabling Multiple Context Mode, page 10-9](#)
- [Configuring Resource Classes, page 10-10](#)
- [Configuring Security Contexts, page 10-16](#)

Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts.

This section provides an overview of security contexts, and includes the following topics:

- [Common Uses for Security Contexts, page 10-2](#)
- [Unsupported Features, page 10-2](#)
- [Context Configuration Files, page 10-2](#)
- [How the Security Appliance Classifies Packets, page 10-2](#)
- [Management Access to Security Contexts, page 10-8](#)

Common Uses for Security Contexts

You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell security services to many customers. By enabling multiple security contexts on the security appliance, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
- You are a large enterprise or a college campus and want to keep departments completely separate.
- You are an enterprise that wants to provide distinct security policies to different departments.
- You have any network that requires more than one security appliance.

Unsupported Features

Multiple context mode does not support the following features:

- Dynamic routing protocols

Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.

- VPN
- Multicast routing. Multicast bridging is supported.
- Threat Detection

Context Configuration Files

Each context has its own configuration file that identifies the security policy, interfaces, and, for supported features, all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

In addition to individual security contexts, the security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts. Like the single mode configuration, this configuration resides as the startup configuration.

The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from a server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only. If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called `admin.cfg`. This context is named “admin.” If you do not want to use `admin.cfg` as the admin context, you can change the admin context.

How the Security Appliance Classifies Packets

Each packet that enters the security appliance must be classified, so that the security appliance can determine to which context to send a packet. This section includes the following topics:

- [Valid Classifier Criteria, page 10-3](#)

- [Invalid Classifier Criteria, page 10-4](#)
- [Classification Examples, page 10-4](#)

**Note**

If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each context.

Valid Classifier Criteria

This section describes the criteria used by the classifier, and includes the following topics:

- [Unique Interfaces, page 10-3](#)
- [Unique MAC Addresses, page 10-3](#)
- [NAT Configuration, page 10-3](#)

Unique Interfaces

If only one context is associated with the ingress interface, the security appliance classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses the interface MAC address. The security appliance lets you assign a different MAC address in each context to the same shared interface, whether it is a shared physical interface or a shared subinterface. By default, shared interfaces do not have unique MAC addresses; the interface uses the physical interface burned-in MAC address in every context. An upstream router cannot route directly to a context without unique MAC addresses. You can set the MAC addresses manually when you configure each interface (see the [“Configuring an Interface \(Single Mode\)” section on page 7-5](#)), or you can automatically generate MAC addresses (see the [“Automatically Assigning MAC Addresses” section on page 10-17](#)).

NAT Configuration

If you do not have unique MAC addresses, then the classifier intercepts the packet and performs a destination IP address lookup. All other fields are ignored; only the destination IP address is used. To use the destination address for classification, the classifier must have knowledge about the subnets located behind each security context. The classifier relies on the NAT configuration to determine the subnets in each context. The classifier matches the destination IP address to either a **static** command or a **global** command. In the case of the **global** command, the classifier does not need a matching **nat** command or an active NAT session to classify the packet. Whether the packet can communicate with the destination IP address after classification depends on how you configure NAT and NAT control.

For example, the classifier gains knowledge about subnets 10.10.10.0, 10.20.10.0 and 10.30.10.0 when the context administrators configure **static** commands in each context:

- Context A:

```
static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0
```
- Context B:

```
static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0
```
- Context C:

```
static (inside,shared) 10.30.10.0 10.30.10.0 netmask 255.255.255.0
```

**Note**

For management traffic destined for an interface, the interface IP address is used for classification.

Invalid Classifier Criteria

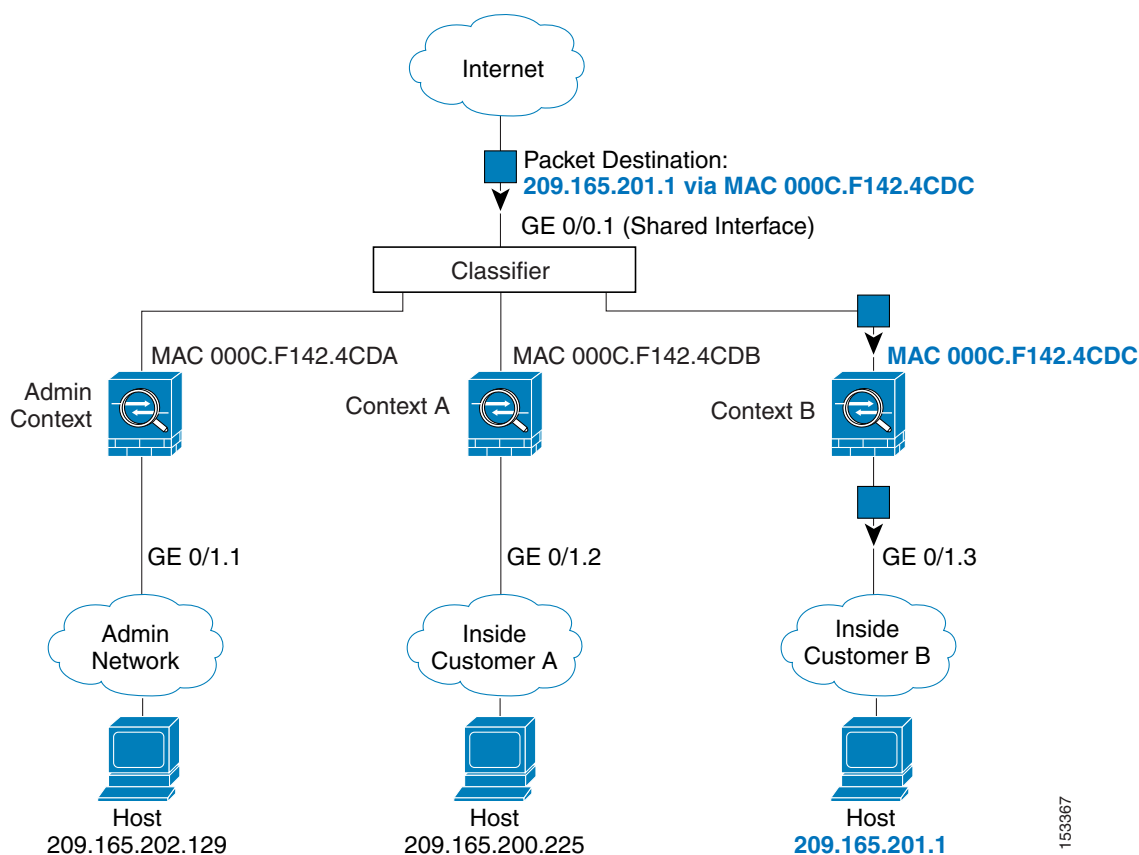
The following configurations are not used for packet classification:

- NAT exemption—The classifier does not use a NAT exemption configuration for classification purposes because NAT exemption does not identify a mapped interface.
- Routing table—If a context includes a static route that points to an external router as the next-hop to a subnet, and a different context includes a **static** command for the same subnet, then the classifier uses the **static** command to classify packets destined for that subnet and ignores the static route.

Classification Examples

Figure 10-1 shows multiple contexts sharing an outside interface. The classifier assigns the packet to Context B because Context B includes the MAC address to which the router sends the packet.

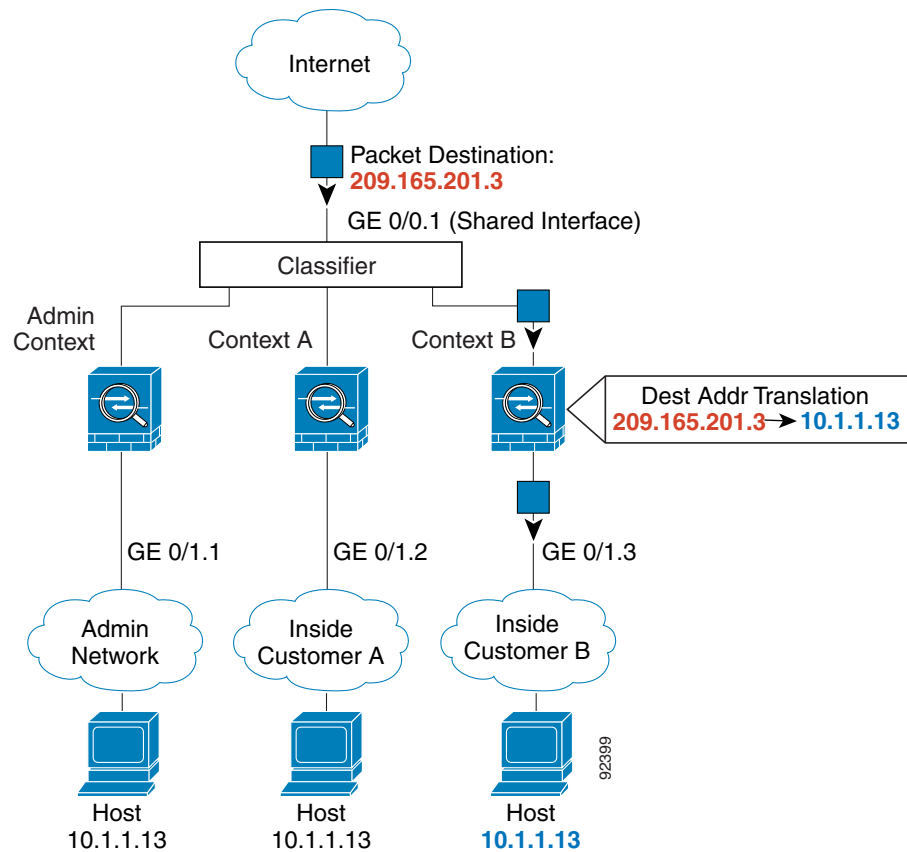
Figure 10-1 Packet Classification with a Shared Interface using MAC Addresses



153367

Figure 10-2 shows multiple contexts sharing an outside interface without MAC addresses assigned. The classifier assigns the packet to Context B because Context B includes the address translation that matches the destination address.

Figure 10-2 Packet Classification with a Shared Interface using NAT

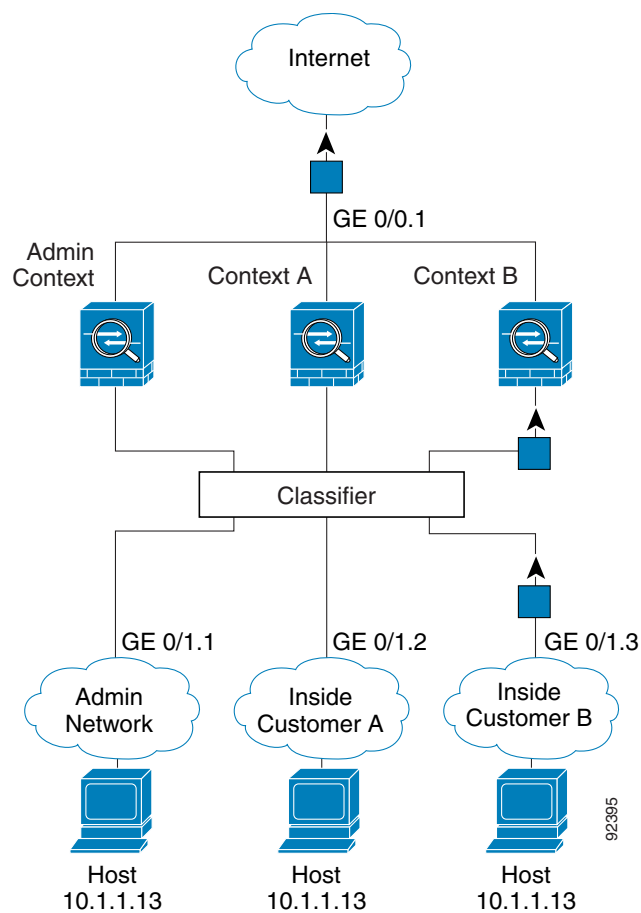


Note that all new incoming traffic must be classified, even from inside networks. Figure 10-3 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 0/1.3, which is assigned to Context B.



Note

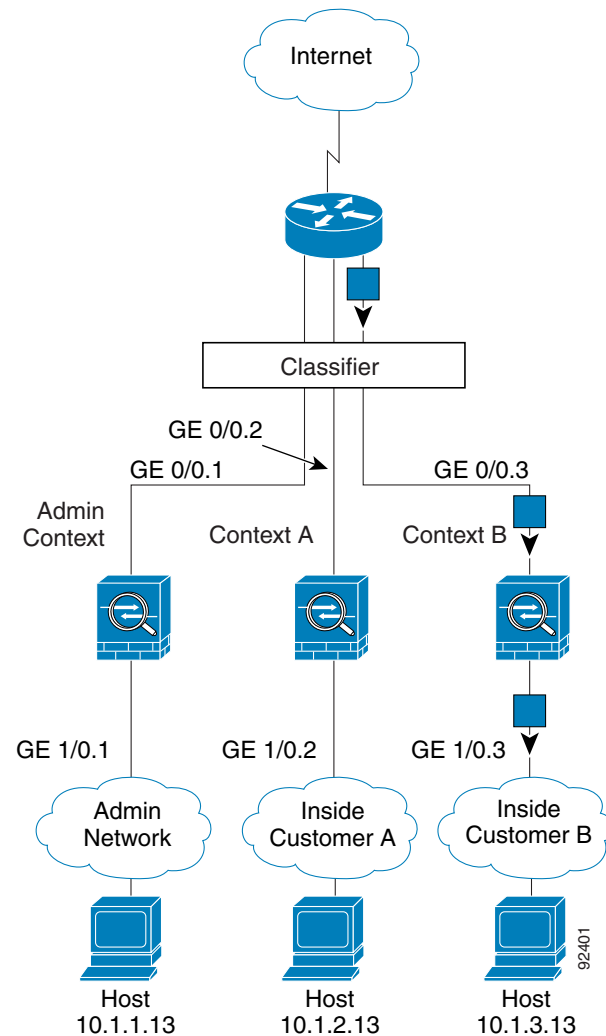
If you share an *inside* interface and do not use unique MAC addresses, the classifier imposes some major restrictions. The classifier relies on the address translation configuration to classify the packet within a context, and you must translate the *destination* addresses of the traffic. Because you do not usually perform NAT on outside addresses, sending packets from inside to outside on a shared interface is not always possible; the outside network is large, (the Web, for example), and addresses are not predictable for an outside NAT configuration. If you share an inside interface, we suggest you use unique MAC addresses.

Figure 10-3 Incoming Traffic from Inside Networks

92395

For transparent firewalls, you must use unique interfaces. Figure 10-4 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 1/0.3, which is assigned to Context B.

Figure 10-4 Transparent Firewall Contexts



Cascading Security Contexts

Placing a context directly in front of another context is called cascading contexts; the outside interface of one context is the same interface as the inside interface of another context. You might want to cascade contexts if you want to simplify the configuration of some contexts by configuring shared parameters in the top context.

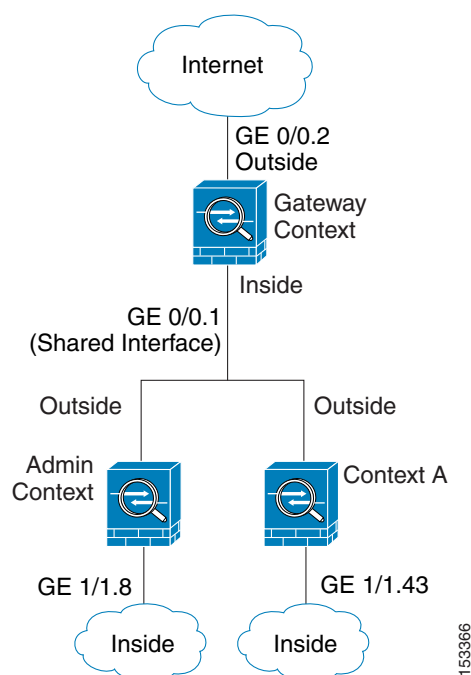


Note

Cascading contexts requires that you configure unique MAC addresses for each context interface. Because of the limitations of classifying packets on shared interfaces without MAC addresses, we do not recommend using cascading contexts without unique MAC addresses.

Figure 10-5 shows a gateway context with two contexts behind the gateway.

Figure 10-5 Cascading Contexts



Management Access to Security Contexts

The security appliance provides system administrator access in multiple context mode as well as access for individual context administrators. The following sections describe logging in as a system administrator or as a context administrator:

- [System Administrator Access, page 10-8](#)
- [Context Administrator Access, page 10-9](#)

System Administrator Access

You can access the security appliance as a system administrator in two ways:

- Access the security appliance console.
From the console, you access the system execution space.
- Access the admin context using Telnet, SSH, or ASDM.

See [Configuring Authentication for Network Access, page 23-1](#) to enable Telnet, SSH, and ASDM access.

As the system administrator, you can access all contexts.

When you change to a context from admin or the system, your username changes to the default “enable_15” username. If you configured command authorization in that context, you need to either configure authorization privileges for the “enable_15” user, or you can log in as a different name for which you provide sufficient privileges in the command authorization configuration for the context. To

log in with a username, enter the **login** command. For example, you log in to the admin context with the username “admin.” The admin context does not have any command authorization configuration, but all other contexts include command authorization. For convenience, each context configuration includes a user “admin” with maximum privileges. When you change from the admin context to context A, your username is altered, so you must log in again as “admin” by entering the **login** command. When you change to context B, you must again enter the **login** command to log in as “admin.”

The system execution space does not support any AAA commands, but you can configure its own enable password, as well as usernames in the local database to provide individual logins.

Context Administrator Access

You can access a context using Telnet, SSH, or ASDM. If you log in to a non-admin context, you can only access the configuration for that context. You can provide individual logins to the context. See [Configuring Authentication for Network Access, page 23-1](#) to enable Telnet, SSH, and SDM access and to configure management authentication.

Enabling or Disabling Multiple Context Mode

Your security appliance might already be configured for multiple security contexts depending on how you ordered it from Cisco. If you are upgrading, however, you might need to convert from single mode to multiple mode by following the procedures in this section.

ASDM supports changing modes from single to multiple mode if you use the High Availability and Scalability Wizard and you enable Active/Active failover. See the [“Accessing and Using the High Availability and Scalability Wizard” section on page 15-4](#) for more information.

If you do not want to use Active/Active failover or want to change back to single mode, you must change modes at the CLI. This section describes changing modes at the CLI, and includes the following topics:

- [Backing Up the Single Mode Configuration, page 10-9](#)
- [Enabling Multiple Context Mode, page 10-9](#)
- [Restoring Single Context Mode, page 10-10](#)

Backing Up the Single Mode Configuration

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files. The original startup configuration is not saved, so if it differs from the running configuration, you should back it up before proceeding.

Enabling Multiple Context Mode

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The

original running configuration is saved as `old_running.cfg` (in the root directory of the internal Flash memory). The original startup configuration is not saved. The security appliance automatically adds an entry for the admin context to the system configuration with the name “admin.”

To enable multiple mode, enter the following command:

```
hostname(config)# mode multiple
```

You are prompted to reboot the security appliance.

Restoring Single Context Mode

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the security appliance; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device. Because the system configuration does not have any network interfaces as part of its configuration, you must access the security appliance from the console to perform the copy.

To copy the old running configuration to the startup configuration and to change the mode to single mode, perform the following steps in the system execution space:

-
- Step 1** To copy the backup version of your original running configuration to the current startup configuration, enter the following command in the system execution space:

```
hostname(config)# copy flash:old_running.cfg startup-config
```



Note

Be sure that you do not save the current running configuration, or it will overwrite the one you just copied.

- Step 2** To set the mode to single mode, enter the following command in the system execution space:

```
hostname(config)# mode single
```

The security appliance reboots.

Configuring Resource Classes

By default, all security contexts have unlimited access to the resources of the security appliance, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

This section includes the following topics:

- [Classes and Class Members Overview, page 10-11](#)
- [Adding a Resource Class, page 10-13](#)
- [Monitoring Context Resource Usage, page 10-15](#)

Classes and Class Members Overview

The security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class. This section includes the following topics:

- [Resource Limits](#), page 10-11
- [Default Class](#), page 10-12
- [Class Members](#), page 10-13

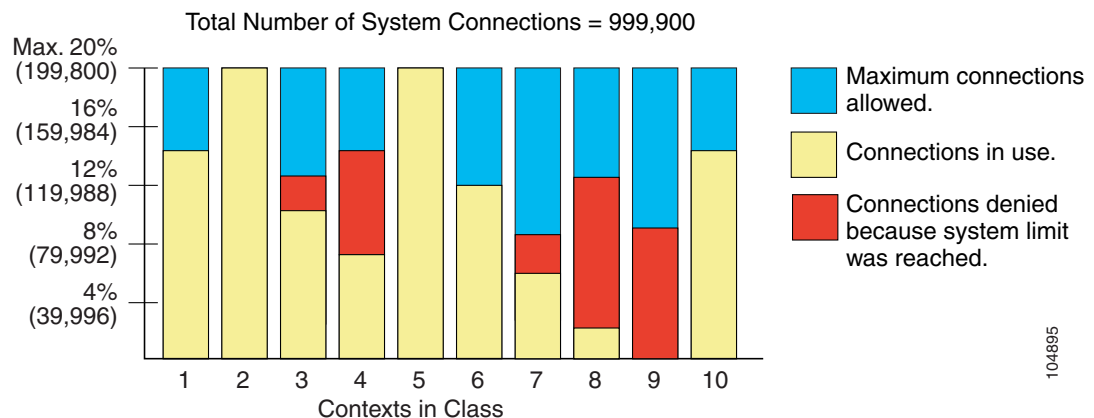
Resource Limits

When you create a class, the security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the security appliance sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can “use up” those resources, potentially affecting service to other contexts.

You can set the limit for individual resources, as a percentage (if there is a hard system limit) or as an absolute value.

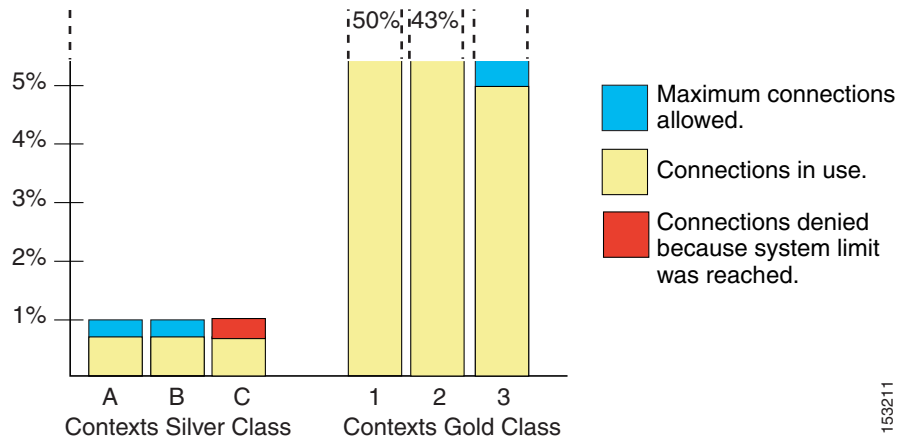
You can oversubscribe the security appliance by assigning more than 100 percent of a resource across all contexts. For example, you can set the Bronze class to limit connections to 20 percent per context, and then assign 10 contexts to the class for a total of 200 percent. If contexts concurrently use more than the system limit, then each context gets less than the 20 percent you intended. (See [Figure 10-6](#).)

Figure 10-6 *Resource Oversubscription*



If you assign an absolute value to a resource across all contexts that exceeds the practical limit of the security appliance, then the performance of the security appliance might be impaired.

The security appliance lets you assign unlimited access to one or more resources in a class, instead of a percentage or absolute number. When a resource is unlimited, contexts can use as much of the resource as the system has available or that is practically available. For example, Context A, B, and C are in the Silver Class, which limits each class member to 1 percent of the connections, for a total of 3 percent; but the three contexts are currently only using 2 percent combined. Gold Class has unlimited access to connections. The contexts in the Gold Class can use more than the 97 percent of “unassigned” connections; they can also use the 1 percent of connections not currently in use by Context A, B, and C, even if that means that Context A, B, and C are unable to reach their 3 percent combined limit. (See [Figure 10-7](#).) Setting unlimited access is similar to oversubscribing the security appliance, except that you have less control over how much you oversubscribe the system.

Figure 10-7 Unlimited Resources

153211

Default Class

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

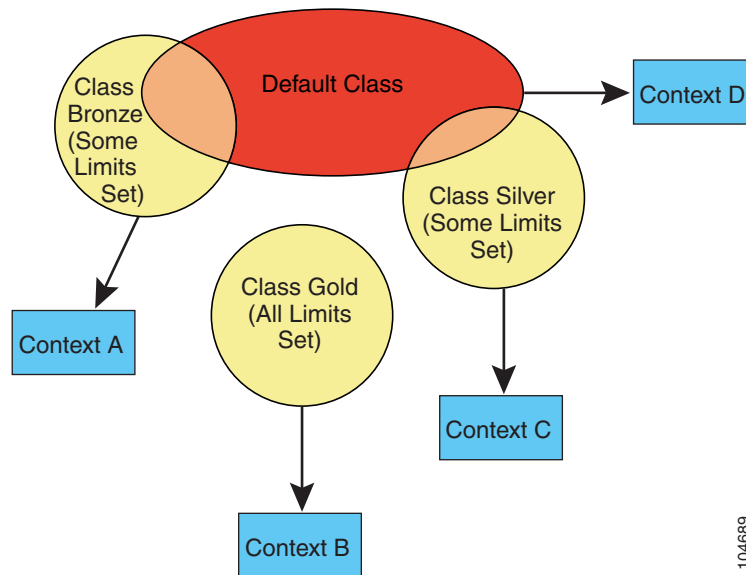
If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with a limit for all resources, the class uses no settings from the default class.

By default, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- IPSec sessions—5 sessions.
- MAC addresses—65,535 entries.

Figure 10-8 shows the relationship between the default class and other classes. Contexts A and C belong to classes with some limits set; other limits are inherited from the default class. Context B inherits no limits from default because all limits are set in its class, the Gold class. Context D was not assigned to a class, and is by default a member of the default class.

Figure 10-8 Resource Classes



Class Members

To use the settings of a class, assign the context to the class when you define the context. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to default. You can only assign a context to one resource class. The exception to this rule is that limits that are undefined in the member class are inherited from the default class; so in effect, a context could be a member of default plus another class.

Adding a Resource Class

For more information about resource classes, see the [“Classes and Class Members Overview”](#) section on page 10-11.

To add a resource class, perform the following steps:

- Step 1** If you are not already in the System configuration mode, in the Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Resource Class pane, click **Add**.
The Add Resource Class dialog box appears.
- Step 3** In the Resource Class field, enter a class name up to 20 characters in length.
- Step 4** In the Count Limited Resources area, set the concurrent limits for resources.

For resources that do not have a system limit, you cannot set the percentage; you can only set an absolute value. If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then the resource is unlimited, or the system limit if available.

You can set one or more of the following limits:

- **Hosts**—Sets the limit for concurrent hosts that can connect through the security appliance. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **Telnet**—Sets the limit for concurrent Telnet sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
- **ASDM Sessions**—Sets the limit for concurrent ASDM sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 80 sessions divided between all contexts. ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts.
- **Connections**—Sets the limit for concurrent TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and the system limit for your model, and selecting **Absolute** from the list. See the *Cisco ASDM Release Notes* for the connection limit for your model.
- **Xlates**—Sets the limit for address translations. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **SSH**—Sets the limit for SSH sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
- **MAC Entries**—(Transparent mode only) Sets the limit for MAC address entries in the MAC address table. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and 65535 and selecting **Absolute** from the list.

Step 5 In the Rate Limited Resources area, set the rate limit for resources.

If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then it is unlimited by default.

You can set one or more of the following limits:

- **Conns/sec**—Sets the limit for connections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **Syslogs/sec**—Sets the limit for system log messages per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.

- **Inspects/sec**—Sets the limit for application inspections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.

Step 6 Click **OK**.

Monitoring Context Resource Usage

To monitor resource usage of all contexts from the system execution space, perform the following steps:

Step 1 If you are not already in the System mode, in the Device List pane, double-click **System** under the active device IP address.

Step 2 Click the **Monitoring** button on the toolbar.

Step 3 Click **Context Resource Usage**.

Click each resource type to view the resource usage for all contexts:

- **ASDM**—Shows the usage of ASDM connections.
 - **Context**—Shows the name of each context.
 - **Existing Connections (#)**—Shows the number of existing connections.
 - **Existing Connections (%)**—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
 - **Peak Connections (#)**—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Telnet**—Shows the usage of Telnet connections.
 - **Context**—Shows the name of each context.
 - **Existing Connections (#)**—Shows the number of existing connections.
 - **Existing Connections (%)**—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
 - **Peak Connections (#)**—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **SSH**—Shows the usage of SSH connections.
 - **Context**—Shows the name of each context.
 - **Existing Connections (#)**—Shows the number of existing connections.
 - **Existing Connections (%)**—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
 - **Peak Connections (#)**—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Xlates**—Shows the usage of network address translations.
 - **Context**—Shows the name of each context.
 - **Xlates (#)**—Shows the number of current xlates.
 - **Xlates (%)**—Shows the xlates used by this context as a percentage of the total number of xlates used by all contexts.

- Peak (#)—Shows the peak number of xlates since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **NATs**—Shows the number of NAT rules.
 - Context—Shows the name of each context.
 - NATs (#)—Shows the current number of NAT rules.
 - NATs (%)—Shows the NAT rules used by this context as a percentage of the total number of NAT rules used by all contexts.
 - Peak NATs (#)—Shows the peak number of NAT rules since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Syslogs**—Shows the rate of system log messages.
 - Context—Shows the name of each context.
 - Syslog Rate (#/sec)—Shows the current rate of system log messages.
 - Syslog Rate (%)—Shows the system log messages generated by this context as a percentage of the total number of system log messages generated by all contexts.
 - Peak Syslog Rate (#/sec)—Shows the peak rate of system log messages since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.

Step 4 Click **Refresh** to refresh the view.

Configuring Security Contexts

This section describes how to add security contexts, and includes the following topics:

- [Adding a Security Context, page 10-16](#)
- [Automatically Assigning MAC Addresses, page 10-17](#)

For more information about security contexts, see the “[Security Context Overview](#)” section on [page 10-1](#).

Adding a Security Context

For more information about security contexts, see the “[Security Context Overview](#)” section on [page 10-1](#).

To add a security context, perform the following steps:

-
- Step 1** If you are not already in the System configuration mode, in the Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Security Contexts pane, click **Add**.
The Add Context dialog box appears.
- Step 3** In the Security Context field, enter the context name as a string up to 32 characters long.
This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. “System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.
- Step 4** In the Interface Allocation area, click the **Add** button to assign an interface to the context.

- Step 5** From the Interfaces > Physical Interface drop-down list, choose an interface.
- You can assign the main interface, in which case you leave the subinterface ID blank, or you can assign a subinterface or a range of subinterfaces associated with this interface. In transparent firewall mode, only interfaces that have not been allocated to other contexts are shown. If the main interface was already assigned to another context, then you must choose a subinterface.
- Step 6** (Optional) In the Interfaces > Subinterface Range (optional) drop-down list, choose a subinterface ID.
- For a range of subinterface IDs, choose the ending ID in the second drop-down list, if available.
- In transparent firewall mode, only subinterfaces that have not been allocated to other contexts are shown.
- Step 7** (Optional) In the Aliased Names area, check **Use Aliased Name in Context** to set an aliased name for this interface to be used in the context configuration instead of the interface ID.
- In the Name field, sets the aliased name.
- An aliased name must start with a letter, end with a letter, and have as interior characters only letters, digits, or an underscore. This field lets you specify a name that ends with a letter or underscore; to add an optional digit after the name, set the digit in the Range field.
- (Optional) In the Range field, set the numeric suffix for the aliased name.
- If you have a range of subinterfaces, you can enter a range of digits to be appended to the name.
- Step 8** (Optional) To enable context users to see physical interface properties even if you set an aliased name, check **Show Hardware Properties in Context**.
- Step 9** Click **OK** to return to the Add Context dialog box.
- Step 10** (Optional) If you use IPS virtual sensors, then assign a sensor to the context in the IPS Sensor Allocation area.
- For detailed information about IPS and virtual sensors, see [Chapter 28, “Configuring IPS.”](#)
- Step 11** (Optional) To assign this context to a resource class, choose a class name from the Resource Assignment > Resource Class drop-down list.
- You can add or edit a resource class directly from this area. See the [“Configuring Resource Classes” section on page 10-10](#) for more information.
- Step 12** To set the context configuration location, identify the URL by choosing a file system type from the Config URL drop-down list and entering a path in the field.
- For example, the combined URL for FTP has the following format:
- ```
ftp://server.example.com/configs/admin.cfg
```
- Step 13** (Optional) For external filesystems, set the username and password by clicking **Login**.
- Step 14** (Optional) To set the failover group for active/active failover, choose the group name in the Failover Group drop-down list.
- Step 15** (Optional) Add a description in the Description field.
- 

## Automatically Assigning MAC Addresses

This section describes how to assign unique MAC addresses to context interfaces, and includes the following sections:

- [MAC Address Overview, page 10-18](#)

- [Enabling Automatic MAC Address Assignment, page 10-18](#)

## MAC Address Overview

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the [“How the Security Appliance Classifies Packets” section on page 10-2](#) for information about classifying packets.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For use with failover, the security appliance generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption.

When you assign an interface to a context, the new MAC address is generated immediately. If you enable this option after you create context interfaces, then MAC addresses are generated for all interfaces immediately after you apply the option. If you disable this option, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

The MAC address is generated using the following format:

- Active unit MAC address: *12\_slot.port\_subid.contextid*.
- Standby unit MAC address: *02\_slot.port\_subid.contextid*.

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

- Active: 1200.0131.0001
- Standby: 0200.0131.0001

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the [“Configuring an Interface \(Single Mode\)” section on page 7-5](#) to manually set the MAC address.

## Enabling Automatic MAC Address Assignment

To enable automatic MAC address assignment, perform the following steps.

- 
- |               |                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | If you are not already in the System configuration mode, in the Device List pane, double-click <b>System</b> under the active device IP address. |
| <b>Step 2</b> | On the Context Management > Security Contexts pane, check <b>Mac-Address auto</b> .                                                              |
-



# CHAPTER 11

## Configuring Dynamic And Static Routing

---

To configure static routes and dynamic routing protocols, go to **Configuration > Device Setup > Routing** area of the ASDM interface.

You can configure up to two OSPF, one EIGRP, and one RIP routing process on the security appliance at the same time. Dynamic routing is only available on security appliances in routed firewall mode; you cannot configure dynamic routing protocols on a security appliance in transparent firewall mode.

You can configure static routes on security appliances in either routed or transparent firewall mode. You can use the static route tracking feature to have the security appliance a backup static route if a primary static route becomes unavailable.

This section contains the following topics:

- [Dynamic Routing, page 11-1](#)
- [Static Routes, page 11-40](#)
- [ASR Group, page 11-45](#)
- [Proxy ARPs, page 11-46](#)

## Dynamic Routing

This section contains the following topics:

- [OSPF, page 11-1](#)
- [RIP, page 11-22](#)
- [EIGRP, page 11-28](#)

## OSPF

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than RIP networks.

OSPF supports MD5 and clear text neighbor authentication. Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (like RIP) can potentially be used by attackers to subvert routing information.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses LSAs to send information about available routes to other OSPF routers. Using ABR type 3 LSA filtering, you can have separate private and public areas with the security appliance acting as an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other. This lets you use NAT and OSPF together without advertising private networks.

**Note**

Only type 3 LSAs can be filtered. If you configure the security appliance as an ASBR in a private network, it will send type 5 LSAs describing private networks, which will get flooded to the entire AS including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either as default or type 5 AS External LSAs. However, you need to configure static routes for the private networks protected by the security appliance. Also, you should not mix public and private networks on the same security appliance interface.

You can have two OSPF routing processes, one RIP routing process, and one EIGRP routing process running on the security appliance at the same time.

For more information about enabling and configuring OSPF, see the following:

- [Setup, page 11-2](#)
- [Filtering, page 11-8](#)
- [Interface, page 11-10](#)
- [Redistribution, page 11-14](#)
- [Static Neighbor, page 11-17](#)
- [Summary Address, page 11-18](#)
- [Virtual Link, page 11-19](#)

## Setup

The Setup pane lets you enable OSPF processes, configure OSPF areas and networks, and define OSPF route summarization.

For more information about configuring these areas, see the following:

- [Setup > Process Instances Tab, page 11-3](#)
- [Setup > Area/Networks Tab, page 11-5](#)
- [Setup > Route Summarization Tab, page 11-7](#)

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Setup > Process Instances Tab

You can enable up to two OSPF process instances. Each OSPF process has its own associated areas and networks.

### Fields

- OSPF Process 1 and 2 areas—Each area contains the settings for a specific OSPF process.
- Enable this OSPF Process—Check the check box to enable an OSPF process. Uncheck this check box to remove the OSPF process.
- OSPF Process ID—Enter a unique numeric identifier for the OSPF process. This process ID is used internal and does not need to match the OSPF process ID on any other OSPF devices. Valid values are from 1 to 65535.
- Advanced—Opens the Edit OSPF Process Advanced Properties dialog box, where you can configure the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings. See [Edit OSPF Process Advanced Properties, page 11-3](#) for more information.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit OSPF Process Advanced Properties

You can edit process-specific settings, such as the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings, in the Edit OSPF Process Advanced Properties dialog box.

### Fields

- OSPF Process—Displays the OSPF process you are configuring. You cannot change this value.
- Router ID—To use a fixed router ID, enter a router ID in IP address format in the Router ID field. If you leave this value blank, the highest-level IP address on the security appliance is used as the router ID.
- Ignore LSA MOSPF—Check this check box to suppress the sending of system log messages when the security appliance receives type 6 (MOSPF) LSA packets. This setting is unchecked by default.

- **RFC 1583 Compatible**—Check this check box to calculate summary route costs per RFC 1583. Uncheck this check box to calculate summary route costs per RFC 2328. To minimize the chance of routing loops, all OSPF devices in an OSPF routing domain should have RFC compatibility set identically. This setting is selected by default.
- **Adjacency Changes**—Contains settings that define the adjacency changes that cause system log messages to be sent.
  - **Log Adjacency Changes**—Check this check box to cause the security appliance to send a system log message whenever an OSPF neighbor goes up or down. This setting is selected by default.
  - **Log Adjacency Changes Detail**—Check this check box to cause the security appliance to send a system log message whenever any state change occurs, not just when a neighbor goes up or down. This setting is unchecked by default.
- **Administrative Route Distances**—Contains the settings for the administrative distances of routes based on the route type.
  - **Inter Area**—Sets the administrative distance for all routes from one area to another. Valid values range from 1 to 255. The default value is 100.
  - **Intra Area**—Sets the administrative distance for all routes within an area. Valid values range from 1 to 255. The default value is 100.
  - **External**—Sets the administrative distance for all routes from other routing domains that are learned through redistribution. Valid values range from 1 to 255. The default value is 100.
- **Timers**—Contains the settings used to configure LSA pacing and SPF calculation timers.
  - **SPF Delay Time**—Specifies the time between when OSPF receives a topology change and when the SPF calculation starts. Valid values range from 0 to 65535. The default value is 5.
  - **SPF Hold Time**—Specifies the hold time between consecutive SPF calculations. Valid values range from 1 to 65534. The default value is 10.
  - **LSA Group Pacing**—Specifies the interval at which LSAs are collected into a group and refreshed, checksummed, or aged. Valid values range from 10 to 1800. The default value is 240.
- **Default Information Originate**—Contains the settings used by an ASBR to generate a default external route into an OSPF routing domain.
  - **Enable Default Information Originate**—Check this check box to enable the generation of the default route into the OSPF routing domain.
  - **Always advertise the default route**—Check this check box to always advertise the default route. This option is unchecked by default.
  - **Metric Value**—Specifies the OSPF default metric. Valid values range from 0 to 16777214. The default value is 1.
  - **Metric Type**—Specifies the external link type associated with the default route advertised into the OSPF routing domain. Valid values are 1 or 2, indicating a Type 1 or a Type 2 external route. The default value is 2.
  - **Route Map**—(Optional) The name of the route map to apply. The routing process generates the default route if the route map is satisfied.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Setup > Area/Networks Tab

The Area/Networks tab displays the areas, and the networks they contain, for each OSPF process on the security appliance.

### Fields

- Area/Networks—Displays information about the areas and the area networks configured for each OSPF process. Double-clicking a row in the table opens the [Add/Edit OSPF Area](#) dialog box for the selected area.
  - OSPF Process—Displays the OSPF process the area applies to.
  - Area ID—Displays the area ID.
  - Area Type—Displays the area type. The area type is one of the following values: Normal, Stub, NSSA.
  - Networks—Displays the area networks.
  - Authentication—Displays the type of authentication set for the area. The authentication type is one of the following values: None, Password, MD5.
  - Options—Displays any options set for the area type.
  - Cost—Displays the default cost for the area.
- Add—Opens the [Add/Edit OSPF Area](#) dialog box. Use this button to add a new area configuration.
- Edit—Opens the [Add/Edit OSPF Area](#) dialog box. Use this button to change the parameters of the selected area.
- Delete—Removes the selected area from the configuration.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit OSPF Area

You define area parameters, the networks contained by the area, and the OSPF process associated with the area in the Add/Edit OSPF Area dialog box.

**Fields**

- **OSPF Process**—When adding a new area, choose the OSPF process ID for the OSPF process for which the area is being. If there is only one OSPF process enabled on the security appliance, then that process is selected by default. When editing an existing area, you cannot change the OSPF process ID.
- **Area ID**—When adding a new area, enter the area ID. You can specify the area ID as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295. You cannot change the area ID when editing an existing area.
- **Area Type**—Contains the settings for the type of area being configured.
  - **Normal**—Choose this option to make the area a standard OSPF area. This option is selected by default when you first create an area.
  - **Stub**—Choosing this option makes the area a stub area. Stub areas do not have any routers or areas beyond it. Stub areas prevent AS External LSAs (type 5 LSAs) from being flooded into the stub area. When you create a stub area, you have the option of preventing summary LSAs (type 3 and 4) from being flooded into the area by unchecking the Summary check box.
  - **Summary**—When the area being defined is a stub area, unchecking this check box prevents LSAs from being sent into the stub area. This check box is selected by default for stub areas.
  - **NSSA**—Choose this option to make the area a not-so-stubby area. NSSAs accept type 7 LSAs. When you create a NSSA, you have the option of preventing summary LSAs from being flooded into the area by unchecking the Summary check box. You can also disable route redistribution by unchecking the Redistribute check box and enabling Default Information Originate.
  - **Redistribute**—Uncheck this check box to prevent routes from being imported into the NSSA. This check box is selected by default.
  - **Summary**—When the area being defined is a NSSA, unchecking this check box prevents LSAs from being sent into the stub area. This check box is selected by default for NSSAs.
  - **Default Information Originate**—Check this check box to generate a type 7 default into the NSSA. This check box is unchecked by default.
  - **Metric Value**—Specifies the OSPF metric value for the default route. Valid values range from 0 to 16777214. The default value is 1.
  - **Metric Type**—The OSPF metric type for the default route. The choices are 1 (type 1) or 2 (type 2). The default value is 2.
- **Area Networks**—Contains the settings for defining an OSPF area.
  - **Enter IP Address and Mask**—Contains the settings used to define the networks in the area.
    - IP Address**—Enter the IP address of the network or host to be added to the area. Use 0.0.0.0 with a netmask of 0.0.0.0 to create the default area. You can only use 0.0.0.0 in one area.
    - Netmask**—Choose the network mask for the IP address or host to be added to the area. If adding a host, choose the 255.255.255.255 mask.
  - **Add**—Adds the network defined in the Enter IP Address and Mask area to the area. The added network appears in the Area Networks table.
  - **Delete**—Deletes the selected network from the Area Networks table.
  - **Area Networks**—Displays the networks defined for the area.
    - IP Address**—Displays the IP address of the network.
    - Netmask**—Displays the network mask for the network.
- **Authentication**—Contains the settings for OSPF area authentication.



- None—Choose this option to disable OSPF area authentication. This is the default setting.
- Password—Choose this option to use a clear text password for area authentication. This option is not recommended where security is a concern.
- MD5—Choose this option to use MD5 authentication.
- Default Cost—Specify a default cost for the area. Valid values range from 0 to 65535. The default value is 1.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Setup > Route Summarization Tab

In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range. To define summary address for external routes being redistributed into an OSPF area, see [Summary Address](#).

### Fields

- Route Summarization—Displays information about route summaries defined on the security appliance. Double-clicking a row in the table opens the [Add/Edit Route Summarization](#) dialog box for the selected route summary.
  - OSPF Process—Displays the OSPF process ID for the OSPF process associated with the route summary.
  - Area ID—Displays the area associated with the route summary.
  - IP Address—Displays the summary address.
  - Network Mask—Displays the summary mask.
  - Advertise—Displays “yes” when the route summaries are advertised when they match the address/mask pair or “no” when route summaries are suppressed when they match the address/mask pair.
- Add—Opens the [Add/Edit Route Summarization](#) dialog box. Use this button to define a new route summarization.
- Edit—Opens the [Add/Edit Route Summarization](#) dialog box. Use this button to change the parameters of the selected route summarization.
- Delete—Removes the selected route summarization from the configuration.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Route Summarization

Use the Add Route Summarization dialog box to add a new entry to the Route Summarization table. Use the Edit Route Summarization dialog box to change an existing entry.

### Fields

- **OSPF Process**—Choose the OSPF process the route summary applies to. You cannot change this value when editing an existing route summary entry.
- **Area ID**—Choose the area ID the route summary applies to. You cannot change this value when editing an existing route summary entry.
- **IP Address**—Enter the network address for the routes being summarized.
- **Network Mask**—Choose one of the common network masks from the list or type the mask in the field.
- **Advertise**—Check this check box to set the address range status to “advertise”. This causes type 3 summary LSAs to be generated. Uncheck this check box to suppress the type 3 summary LSA for the specified networks. This check box is checked by default.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Filtering

The Filtering pane displays the ABR type 3 LSA filters that have been configured for each OSPF process.

ABR type 3 LSA filters allow only specified prefixes to be sent from one area to another area and restricts all other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time.

### Benefits

OSPF ABR type 3 LSA filtering improves your control of route distribution between OSPF areas.

### Restrictions

Only type 3 LSAs that originate from an ABR are filtered.

### Fields

The Filtering table displays the following information. Double-clicking a table entry opens the [Add/Edit Filtering Entry](#) dialog box for the selected entry.

- OSPF Process—Displays the OSPF process associated with the filter entry.
- Area ID—Displays the ID of the area associated with the filter entry.
- Filtered Network—Displays the network address being filtered.
- Traffic Direction—Displays “Inbound” if the filter entry applies to LSAs coming in to an OSPF area or Outbound if it applies to LSAs coming out of an OSPF area.
- Sequence #—Displays the sequence number for the filter entry. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
- Action—Displays “Permit” if LSAs matching the filter are allowed or “Deny” if LSAs matching the filter are denied.
- Lower Range—Displays the minimum prefix length to be matched.
- Upper Range—Displays the maximum prefix length to be matched.

You can perform the following actions on entries in the Filtering table:

- Add—Opens the [Add/Edit Filtering Entry](#) dialog box for adding a new entry to the Filter table.
- Edit—Opens the [Add/Edit Filtering Entry](#) dialog box for modifying the selected filter.
- Delete—Removes the selected filter from the Filter table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit Filtering Entry

The Add/Edit Filtering Entry dialog box lets you add new filters to the Filter table or to modify an existing filter. Some of the filter information cannot be changed when you edit an existing filter.

### Fields

- OSPF Process—Choose the OSPF process associated with the filter entry. If you are editing an existing filter entry, you cannot modify this setting.
- Area ID—Choose the ID of the area associated with the filter entry. If you are editing an existing filter entry, you cannot modify this setting.
- Filtered Network—Enter the address and mask of the network being filtered using CIDR notation (a.b.c.d/m).
- Traffic Direction—Choose the traffic direction being filtered. Choose “Inbound” to filter LSAs coming into an OSPF area or “Outbound” to filter LSAs coming out of an OSPF area. If you are editing an existing filter entry, you cannot modify this setting.

- **Sequence #**—Enter a sequence number for the filter. Valid values range from 1 to 4294967294. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
- **Action**—Choose “Permit” to allow the LSA traffic or “Deny” to block the LSA traffic.
- **Optional**—Contains the optional settings for the filter.
  - **Lower Range**—Specify the minimum prefix length to be matched. The value of this setting must be greater than the length of the network mask entered in the Filtered Network field and less than or equal to the value, if present, entered in the Upper Range field.
  - **Upper Range**—Enter the maximum prefix length to be matched. The value of this setting must be greater than or equal to the value, if present, entered in the Lower Range field, or, if the Lower Range field is left blank, greater than the length of the network mask length entered in the Filtered Network field.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Interface

The Interface pane lets you configure interface-specific OSPF routing properties, such as OSPF message authentication and properties. For more information about configuring these properties, see the following:

- [Interface > Authentication Tab](#)
- [Interface > Properties Tab](#)

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Interface > Authentication Tab

The Authentication tab displays the OSPF authentication information for the security appliance interfaces.

### Fields

- **Authentication Properties**—Displays the authentication information for the security appliance interfaces. Double-clicking a row in the table opens the [Edit OSPF Interface Properties](#) dialog box for the selected interface.

- Interface—Displays the interface name.
- Authentication Type—Displays the type of OSPF authentication enabled on the interface. The authentication type can be one of the following values:
  - None—OSPF authentication is disabled.
  - Password—Clear text password authentication is enabled.
  - MD5—MD5 authentication is enabled.
- Area—The authentication type specified for the area is enabled on the interface. Area authentication is the default value for interfaces. However, area authentication is disabled by default. So, unless you previously specified an area authentication type, interfaces showing Area authentication have authentication disabled.
- Edit—Opens the [Edit OSPF Interface Properties](#) dialog box for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Edit OSPF Interface Authentication

The Edit OSPF Interface Authentication dialog box lets you configure the OSPF authentication type and parameters for the selected interface.

#### Fields

- Interface—Displays the name of the interface for which authentication is being configured. You cannot edit this field.
- Authentication—Contains the OSPF authentication options.
  - None—Choose this option to disable OSPF authentication.
  - Password—Choose this option to use clear text password authentication. This is not recommended where security is a concern.
  - MD5—Choose this option to use MD5 authentication (recommended).
  - Area—(Default) Choose this option to use the authentication type specified for the area (see [Add/Edit OSPF Area](#) for information about configuring area authentication). Area authentication is disabled by default. So, unless you have previously specified an area authentication type, interfaces set to area authentication have authentication disabled until you configure area authentication.
- Authentication Password—Contains the settings for entering the password when password authentication is enabled.
  - Enter Password—Enter a text string of up to 8 characters.
  - Re-enter Password—Reenter the password.

- MD5 IDs and Keys—Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID.
  - Enter MD5 ID and Key—Contains the settings for entering MD5 key information.
    - Key ID—Enter a numerical key identifier. Valid values range from 1 to 255.
    - Key—An alphanumeric character string of up to 16 bytes.
  - Add—Adds the specified MD5 key to the MD5 ID and Key table.
  - Delete—Removes the selected MD5 key and ID from the MD5 ID and Key table.
  - MD5 ID and Key—Displays the configured MD5 keys and key IDs.
    - Key ID—Displays the key ID for the selected key.
    - Key—Displays the key for the selected key ID.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Interface > Properties Tab

The Properties tab displays the OSPF properties defined for each interface in a table format.

### Fields

- OSPF Interface Properties—Displays interface-specific OSPF properties. Double-clicking a row in the table opens the [Edit OSPF Interface Properties](#) dialog box for the selected interface.
  - Interface—Displays the name of the interface that the OSPF configuration applies to.
  - Broadcast—Displays “No” if the interface is set to non-broadcast (point-to-point). Displays “Yes” if the interface is set to broadcast. “Yes” is the default setting for Ethernet interfaces.
  - Cost—Displays the cost of sending a packet through the interface.
  - Priority—Displays the OSPF priority assigned to the interface.
  - MTU Ignore—Displays “No” if MTU mismatch detection is enabled. Displays “Yes” if the MTU mismatch detection is disabled.
  - Database Filter—Displays “Yes” if outgoing LSAs are filtered during synchronization and flooding. Displays “No” if filtering is not enabled.
- Edit—Opens the [Edit OSPF Interface Properties](#) dialog box for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit OSPF Interface Properties

### Fields

- Interface—Displays the name of the interface for which you are configuring OSPF properties. You cannot edit this field.
- Broadcast—Check this check box to specify that the interface is a broadcast interface. This check box is selected by default for Ethernet interfaces. Uncheck this check box to designate the interface as a point-to-point, non-broadcast interface. Specifying an interface as point-to-point, non-broadcast lets you transmit OSPF routes over VPN tunnels.

When an interface is configured as point-to-point, non-broadcast, the following restrictions apply:

- You can define only one neighbor for the interface.
- You need to manually configure the neighbor (see [Static Neighbor](#)).
- You need to define a static route pointing to the crypto endpoint (see [Static Routes](#)).
- If OSPF over the tunnel is running on the interface, regular OSPF with an upstream router cannot be run on the same interface.
- You should bind the crypto-map to the interface before specifying the OSPF neighbor to ensure that the OSPF updates are passed through the VPN tunnel. If you bind the crypto-map to the interface after specifying the OSPF neighbor, use the **clear local-host all** command to clear OSPF connections so the OSPF adjacencies can be established over the VPN tunnel.
- Cost—Specify the cost of sending a packet through the interface. The default value is 10.
- Priority—Specify the OSPF router priority. When two routers connect to a network, both attempt to become the designated router. The devices with the higher router priority becomes the designated router. If there is a tie, the router with the higher router ID becomes the designated router.

Valid values for this setting range from 0 to 255. The default value is 1. Entering 0 for this setting makes the router ineligible to become the designated router or backup designated router. This setting does not apply to interfaces that are configured as point-to-point non-broadcast interfaces.

- MTU Ignore—OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.
- Database Filter—Check this check box to filter outgoing LSA interface during synchronization and flooding. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. In a fully meshed topology, this can waste bandwidth and lead to excessive link and CPU usage. Checking this check box prevents flooding OSPF LSA on the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit OSPF Interface Advanced Properties

The Edit OSPF Interface Advanced Properties dialog box lets you change the values for the OSPF hello interval, retransmit interval, transmit delay, and dead interval. Typically, you only need to change these values from the defaults if you are experiencing OSPF problems on your network.

### Fields

- **Hello Interval**—Specifies the interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
- **Retransmit Interval**—Specifies the time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.
- **Transmit Delay**—Specifies the estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.
- **Dead Interval**—Specifies the interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this setting is four times the interval set by the Hello Interval field.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Redistribution

The Redistribution pane displays the rules for redistributing routes from one routing process into an OSPF routing process.



### Fields

The Redistribution table displays the following information. Double-clicking a table entry opens the [Add/Edit OSPF Redistribution Entry](#) dialog box for the selected entry.

- **OSPF Process**—Displays the OSPF process associated with the route redistribution entry.
- **Protocol**—Displays the source protocol the routes are being redistributed from. Valid entries are the following:
  - **Static**—Static routes are redistributed into the OSPF routing process.
  - **Connected**—The route was established automatically by virtue of having IP enabled on the interface. These routes are redistributed into the OSPF routing process as external to the AS.
  - **OSPF**—Routes from another OSPF routing process are being redistributed into the OSPF routing process.
  - **EIGRP**—Routes are redistributed from the EIGRP routing process into the OSPF routing process.
  - **RIP**—Routes are redistributed from the RIP routing process into the OSPF routing process.
- **Match**—Displays the conditions used for redistributing routes from one OSPF routing process to another.
- **Subnets**—Displays “Yes” if subnetted routes are redistributed. Does not display anything if only routes that are not subnetted are redistributed.
- **Metric Value**—Displays the metric that is used for the route. This column is blank for redistribution entries if the default metric is used.
- **Metric Type**—Displays “1” if the metric is a Type 1 external route, “2” if the metric is Type 2 external route.
- **Tag Value**—A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
- **Route Map**—Displays the name of the route map to apply to the redistribution entry.

You can perform the following actions on the Redistribution table entries:

- **Add**—Opens the [Add/Edit OSPF Redistribution Entry](#) dialog box for adding a new redistribution entry.
- **Edit**—Opens the [Add/Edit OSPF Redistribution Entry](#) dialog box for modifying the selected redistribution entry.
- **Delete**—Removes the selected redistribution entry from the Redistribution table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit OSPF Redistribution Entry

The Add/Edit OSPF Redistribution Entry dialog box lets you add a new redistribution rule to or edit an existing redistribution rule in the Redistribution table. Some of the redistribution rule information cannot be changed when you are editing an existing redistribution rule.

### Fields

- **OSPF Process**—Choose the OSPF process associated with the route redistribution entry. If you are editing an existing redistribution rule, you cannot change this setting.
- **Protocol**—Choose the source protocol the routes are being redistributed from. You can choose one of the following options:
  - **Static**—Redistribute static routes into the OSPF routing process.
  - **Connected**—Redistribute connected routes (routes established automatically by virtue of having IP enabled on the interface) into the OSPF routing process. Connected routes are redistributed as external to the AS.
  - **OSPF**—Redistribute routes from another OSPF routing process. Choose the OSPF process ID from the list.
  - **RIP**—Redistribute routes from the RIP routing process.
  - **EIGRP**—Redistribute routes from the EIGRP routing process. Choose the autonomous system number of the EIGRP routing process from the list.
- **Match**—Displays the conditions used for redistributing routes from another OSPF routing process into the selected OSPF routing process. These options are not available when redistributing static, connected, RIP, or EIGRP routes. The routes must match the selected condition to be redistributed. You can choose one or more of the following match conditions:
  - **Internal**—The route is internal to a specific AS.
  - **External 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes.
  - **External 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes.
  - **NSSA External 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.
  - **NSSA External 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.
- **Metric Value**—Specify the metric value for the routes being redistributed. Valid values range from 1 to 16777214. When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
- **Metric Type**—Choose “1” if the metric is a Type 1 external route, “2” if the metric is a Type 2 external route.
- **Tag Value**—The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
- **Use Subnets**—Check this check box to enable the redistribution of subnetted routes. Uncheck this check box to cause only routes that are not subnetted to be redistributed.
- **Route Map**—Enter the name of the route map to apply to the redistribution entry.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Static Neighbor

The Static Neighbor pane displays manually defined neighbors; it does not display discovered neighbors.

You need to define a static neighbor for each point-to-point, non-broadcast interface. You also need to define a static route for each static neighbor in the Static Neighbor table.

### Fields

- **Static Neighbor**—Displays information for the static neighbors defined for each OSPF process. Double-clicking a row in the table opens the [Add/Edit OSPF Neighbor Entry](#) dialog box.
  - **OSPF Process**—Displays the OSPF process associated with the static neighbor.
  - **Neighbor**—Displays the IP address of the static neighbor.
  - **Interface**—Displays the interface associated with the static neighbor.
- **Add**—Opens the [Add/Edit OSPF Neighbor Entry](#) dialog box. Use this button to define a new static neighbor.
- **Edit**—Opens the [Add/Edit OSPF Neighbor Entry](#) dialog box. Use this button to change the settings for a static neighbor.
- **Delete**—Removes the selected entry from the Static Neighbor table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit OSPF Neighbor Entry

The Add/Edit OSPF Neighbor Entry dialog box lets you define a new static neighbor or change information for an existing static neighbor.

You must define a static neighbor for each point-to-point, non-broadcast interface.

### Restrictions

- You cannot define the same static neighbor for two different OSPF processes.
- You need to define a static route for each static neighbor (see [Static Routes](#), page 11-42).

**Fields**

- **OSPF Process**—Choose the OSPF process associated with the static neighbor. If you are editing an existing static neighbor, you cannot change this value.
- **Neighbor**—Enter the IP address of the static neighbor.
- **Interface**—Choose the interface associated with the static neighbor. If you are editing an existing static neighbor, you cannot change this value.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Summary Address

The Summary Address pane displays information about the summary addresses configured for each OSPF routing process.

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. Summary routes help reduce the size of the routing table.

Using summary routes for OSPF causes an OSPF ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by the address. Only routes from other routing protocols that are being redistributed into OSPF can be summarized.

**Fields**

The following information appears in the Summary Address table. Double-clicking an entry in the table opens the [Add/Edit OSPF Summary Address Entry](#) dialog box for the selected entry.

- **OSPF Process**—Displays the OSPF process associated with the summary address.
- **IP Address**—Displays the IP address of the summary address.
- **Netmask**—Displays the network mask of the summary address.
- **Advertise**—Displays “Yes” if the summary routes are advertised. Displays “No” if the summary route is not advertised.
- **Tag**—Displays a 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs.

You can perform the following actions on the entries in the Summary Address table:

- **Add**—Opens the [Add/Edit OSPF Summary Address Entry](#) dialog box for adding new summary address entries.
- **Edit**—Opens the [Add/Edit OSPF Summary Address Entry](#) dialog box for editing the selected entry.
- **Delete**—Removes the selected summary address entry from the Summary Address table.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit OSPF Summary Address Entry

The Add/Edit OSPF Summary Address Entry dialog box lets you add new entries to or modify existing entries in the Summary Address table. Some of the summary address information cannot be changed when editing an existing entry.

#### Fields

- **OSPF Process**—Choose the OSPF process associated with the summary address. You cannot change this information when editing an existing entry.
- **IP Address**—Enter the IP address of the summary address. You cannot change this information when editing an existing entry.
- **Netmask**—Enter the network mask for the summary address, or choose the network mask from the list of common masks. You cannot change this information when editing an existing entry.
- **Advertise**—Check this check box to advertise the summary route. Uncheck this check box to suppress routes that fall under the summary address. By default this check box is checked.
- **Tag**—(Optional) The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Virtual Link

If you add an area to an OSPF network, and it is not possible to connect the area directly to the backbone area, you need to create a virtual link. A virtual link connects two OSPF devices that have a common area, called the transit area. One of the OSPF devices must be connected to the backbone area.

#### Fields

The Virtual Link table displays the following information. Doubling-clicking an entry in the table opens the [Add/Edit Virtual Link](#) dialog box for the selected entry.

- **OSPF Process**—Displays the OSPF process associated with the virtual link.
- **Area ID**—Displays the ID of the transit area.
- **Peer Router ID**—Displays the router ID of the virtual link neighbor.

- Authentication—Displays the type of authentication used by the virtual link:
  - None—No authentication is used.
  - Password—Clear text password authentication is used.
  - MD5—MD5 authentication is used.

You can perform the following actions on the entries in the Virtual Link table:

- Add—Opens the [Add/Edit Virtual Link](#) dialog box for adding a new entry to the Virtual Link table.
- Edit—Opens the [Add/Edit Virtual Link](#) dialog box for the selected entry.
- Delete—Removes the selected entry from the Virtual Link table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit Virtual Link

The Add/Edit Virtual Link dialog box lets you define new virtual links or change the properties of existing virtual links.

### Fields

- OSPF Process—Choose the OSPF process associated with the virtual link. If you are editing an existing virtual link, you cannot change this value.
- Area ID—Choose the area shared by the neighbor OSPF devices. The selected area cannot be an NSSA or a Stub area. If you are editing an existing virtual link, you cannot change this value.
- Peer Router ID—Enter the router ID of the virtual link neighbor. If you are editing an existing virtual link, you cannot change this value.
- Advanced—Opens the [Advanced OSPF Virtual Link Properties](#) dialog box. You can configure the OSPF properties for the virtual link in this area. These properties include authentication and packet interval settings.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Advanced OSPF Virtual Link Properties

The Advanced OSPF Virtual Link Properties dialog box lets you configure OSPF authentication and packet intervals.

### Fields

- Authentication—Contains the OSPF authentication options.
  - None—Choose this option to disable OSPF authentication.
  - Password—Choose this option to use clear text password authentication. This is not recommended where security is a concern.
  - MD5—Choose this option to use MD5 authentication (recommended).
- Authentication Password—Contains the settings for entering the password when password authentication is enabled.
  - Enter Password—Enter a text string of up to 8 characters.
  - Re-enter Password—Reenter the password.
- MD5 IDs and Keys—Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID.
  - Enter MD5 ID and Key—Contains the settings for entering MD5 key information.
    - Key ID—Enter a numerical key identifier. Valid values range from 1 to 255.
    - Key—An alphanumeric character string of up to 16 bytes.
  - Add—Adds the specified MD5 key to the MD5 ID and Key table.
  - Delete—Removes the selected MD5 key and ID from the MD5 ID and Key table.
  - MD5 ID and Key—Displays the configured MD5 keys and key IDs.
    - Key ID—Displays the key ID for the selected key.
    - Key—Displays the key for the selected key ID.
- Intervals—Contains the settings for modifying packet interval timing.
  - Hello Interval—Specifies the interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
  - Retransmit Interval—Specifies the time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.
  - Transmit Delay—Specifies the estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.

- **Dead Interval**—Specifies the interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this field is four times the interval set by the Hello Interval field.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## RIP

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. When RIP is enabled on an interface, the interface exchanges RIP broadcasts with neighboring devices to dynamically learn about and advertise routes.

The security appliance support both RIP version 1 and RIP version 2. RIP version 1 does not send the subnet mask with the routing update. RIP version 2 sends the subnet mask with the routing update and supports variable-length subnet masks. Additionally, RIP version 2 supports neighbor authentication when routing updates are exchanged. This authentication ensures that the security appliance receives reliable routing information from a trusted source.

### Limitations

RIP has the following limitations:

- The security appliance cannot pass RIP updates between interfaces.
- RIP Version 1 does not support variable-length subnet masks.
- RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
- RIP convergence is relatively slow compared to other routing protocols.
- You can only enable a single RIP process on the security appliance.

### RIP Version 2 Notes

The following information applies to RIP Version 2 only:

- If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP version 2 updates to the interface.
- With RIP version 2, the security appliance transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
- When RIP version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP version 2 configuration is removed from an interface, that multicast address is unregistered.



## Setup

Use the Setup pane to enable RIP on the security appliance and to configure global RIP protocol parameters. You can only enable a single RIP process on the security appliance.

### Fields

- **Enable RIP Routing**—Check this check box to enable RIP routing on the security appliance. When you enable RIP, it is enabled on all interfaces. Checking this check box also enables the other fields on this pane. Uncheck this check box to disable RIP routing on the security appliance.
- **Enable Auto-summarization**—Clear this check box to disable automatic route summarization. Check this check box to reenable automatic route summarization. RIP Version 1 always uses automatic summarization. You cannot disable automatic summarization for RIP Version 1. If you are using RIP Version 2, you can turn off automatic summarization by unchecking this check box. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.
- **Enable RIP version**—Check this check box to specify the version of RIP used by the security appliance. If this check box is cleared, then the security appliance sends RIP Version 1 updates and accepts RIP Version 1 & Version 2 updates. This setting can be overridden on a per-interface basis in the [Interface](#) pane.
  - **Version 1**—Specifies that the security appliance only sends and receives RIP Version 1 updates. Any version 2 updates received are dropped.
  - **Version 2**—Specifies that the security appliance only sends and receives RIP Version 2 updates. Any version 1 updates received are dropped.
- **Enable default information originate**—Check this check box to generate a default route into the RIP routing process. You can configure a route map that must be satisfied before the default route can be generated.
  - **Route-map**—Enter the name of the route map to apply. The routing process generates the default route if the route map is satisfied.
- **IP Network to Add**—Defines a network for the RIP routing process. The network number specified must not contain any subnet information. There is no limit to the number of network you can add to the security appliance configuration. RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.
  - **Add**—Click this button to add the specified network to the list of networks.
  - **Delete**—Click this button to removed the selected network from the list of networks.
- **Configure interfaces as passive globally**—Check this check box to set all interfaces on the security appliance to passive RIP mode. The security appliance listens for RIP routing broadcasts on all interfaces and uses that information to populate the routing tables but do not broadcast routing updates. To set specific interfaces to passive RIP, use the Passive Interfaces table.
- **Passive Interfaces table**—Lists the configured interfaces on the security appliance. Check the check box in the Passive column for those interfaces you want to operate in passive mode. The other interfaces will still send and receive RIP broadcasts.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Interface

The Interface pane allows you to configure interface-specific RIP settings, such as the version of RIP the interface sends and receives and the authentication method, if any, used for the RIP broadcasts.

### Fields

- Interface table—Each row displays the interface-specific RIP settings for an interface. Double-clicking a row for that entry opens the [Edit RIP Interface Entry](#) dialog box for that interface.
- Edit—Opens the [Edit RIP Interface Entry](#) dialog box for the interface selected in the Interface table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit RIP Interface Entry

The Edit RIP Interface Entry dialog box allows you to configure the interface-specific RIP settings.

### Fields

- Override Global Send Version—Check this check box to specify the RIP version sent by the interface. You can select the following options:
  - Version 1
  - Version 2
  - Version 1 & 2
 Unchecking this check box restores the global setting.
- Override Global Receive Version—Check this check box to specify the RIP version accepted by the interface. If a RIP updated from an unsupported version of RIP is received by the interface, it is dropped. You can select the following options:
  - Version 1
  - Version 2
  - Version 1 & 2
 Unchecking this check box restores the global setting.

- **Enable Authentication**—Check this check box to enable RIP authentication. Uncheck this check box to disable RIP broadcast authentication.
  - **Key**—The key used by the authentication method. Can contain up to 16 characters.
  - **Key ID**—The key ID. Valid values are from 0 to 255.
  - **Authentication Mode**—You can select the following authentication modes:
    - MD5**—Uses MD5 for RIP message authentication.
    - Text**—Uses cleartext for RIP message authentication (not recommended).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Filter Rules

Filter rules allow you to filter the network received in RIP routing updates or sent in RIP routing updates. Each filter rule consists of one or more network rules.

### Fields

- **Filter Rules table**—Displays the configured RIP filter rules.
- **Add**—Clicking this button opens the [Add/Edit Filter Rule](#) dialog box. The new filter rule is added to the bottom of the list.
- **Edit**—Clicking this button opens the [Add/Edit Filter Rule](#) dialog box for the selected filter rule.
- **Delete**—Clicking this button deletes the selected filter rule.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit Filter Rule

Use the Add/Edit Filter Rule pane to create filter rules. You can create filter rules that apply to all interfaces or that apply to a specific interface.

### Fields

- **Direction**—Select one of the following directions for the filter to act upon:

- In—Filters networks on incoming RIP updates.
- Out—Filters networks from outgoing RIP updates.
- Interface—You can select a specific interface for the filter rule, or you can select the All Interfaces option to apply the filter to all interfaces.
- Action—(*Display only*) Displays Permit if the specified network is not filtered from incoming or outgoing RIP advertisements. Displays Deny if the specified network is to be filtered from incoming or outgoing RIP advertisements.
- IP Address—(*Display only*) Displays the IP address of the network being filtered.
- Netmask—(*Display only*) Displays the network mask applied to the IP address.
- Insert—Click this button to add a network rule above the selected rule in the list. Clicking this button opens the [Network Rule](#) dialog box.
- Edit—Click this button to edit the selected rule. Clicking this button opens the [Network Rule](#) dialog box.
- Add—Click this button to add a network rule below the selected rule in the list. Clicking this button opens the [Network Rule](#) dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Network Rule

The Network Rule pane allows you to configure permit and deny rules for specific networks in a filter rule.

### Fields

- Action—Select Permit to allow the specified network to be advertised in RIP updates or accepted into the RIP routing process. Select Deny to prevent the specified network from being advertised in RIP updates or accepted into the RIP routing process.
- IP Address—Type IP address of the network being permitted or denied.
- Netmask—Specify the network mask applied to the network IP address. You can type a network mask into this field or select one of the common masks from the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Redistribution

The Redistribution pane displays the routes that are being redistributed from other routing processes into the RIP routing process.

### Fields

- Protocol—(*Display only*) Displays the routing protocol being redistributed into the RIP routing process:
  - Static—Static routes.
  - Connected—Directly connected networks.
  - OSPF—Networks discovered by the specified OSPF routing process.
  - EIGRP—Networks discovered by the specified EIGRP routing process.
- Metric—The RIP metric being applied to the redistributed routes.
- Match—(*Display only*) Displays the type of OSPF routes being redistributed into the RIP routing process. If the Match column is blank for an OSPF redistribution rule, Internal, External 1, and External 2 routes are redistributed into the RIP routing process.
- Route Map—(*Display only*) Displays the name of the route map, if any, being applied to the redistribution. Route maps are used to specify with greater detail which routes from the specified routing process are redistributed into RIP.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Route Redistribution

Use the Add Route Redistribution dialog box to add a new redistribution rule. Use the Edit Route Redistribution dialog box to change an existing rule.

### Fields

- Protocol—Choose the routing protocol to redistribute into the RIP routing process:
  - Static—Static routes.
  - Connected—Directly connected networks.

- OSPF and OSPF ID—Routes discovered by the OSPF routing process. If you choose OSPF, you must also enter the OSPF process ID. Additionally, you can select the specific types of OSPF routes to redistribute from the Match area.
- EIGRP and EIGRP ID—Routes discovered by the EIGRP routing process. If you choose EIGRP, you must also specify the autonomous system number of the EIGRP routing process in the EIGRP ID field.
- Route Map—Specifies the name of a route map that must be satisfied before the route can be redistributed into the RIP routing process.
- Configure Metric Type—Check this check box to specify a metric for the redistributed routes. If not specified, the routes are assigned a metric of 0.
  - Transparent—Choose this option to cause the current route metric to be used.
  - Value—Choose this to assign a specific metric value. You can enter a value from 0 to 16.
- Match—If you are redistributing OSPF routes into the RIP routing process, you can choose specific types of OSPF routes to redistribute by checking the check box next to the route type. If you do not check any route types, Internal, External 1, and External 2 routes are redistributed by default.
  - Internal—Routes internal to the AS are redistributed.
  - External 1—Type 1 routes external to the AS are redistributed.
  - External 2—Type 2 routes external to the AS are redistributed.
  - NSSA External 1—Type 1 routes external to an NSSA are redistributed.
  - NSSA External 2—Type 2 routes external to an NSSA are redistributed.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## EIGRP

EIGRP is an enhanced version of IGRP developed by Cisco. Unlike IGRP and RIP, EIGRP does not send out periodic route updates. EIGRP updates are sent out only when the network topology changes.

You can enable only one EIGRP routing process on the security appliance.

This section contains the following information:

- [Configuring EIGRP, page 11-29](#)
- [Field Information for the EIGRP Panes, page 11-30](#)

For information about monitoring dynamically discovered EIGRP neighbors, see [Monitoring EIGRP Neighbors, page 43-7](#).

## Configuring EIGRP

To configure EIGRP routing on the Security Appliance, perform the following steps:

- 
- Step 1** Go to the **Configuration > Device Setup > Routing > EIGRP** area of the ASDM interface.
- Step 2** Enable the EIGRP routing process on the **Setup > Process Instances** tab. See [Process Instances, page 11-30](#) for more information.
- Step 3** (Optional) Configure the EIGRP routing process parameters. Click **Advanced** on the Setup > Process Instances tab.
- You can configure the EIGRP routing process as a stub routing process, disable automatic route summarization, define the default metrics for redistributed routes, change the administrative distances for internal and external EIGRP routes, configure a static router ID, and enable or disable the logging of adjacency changes. See [Edit EIGRP Process Advanced Properties, page 11-31](#) for more information.
- Step 4** Define the networks and interfaces that will participate in EIGRP routing on the **Setup > Networks** tab. See [Networks, page 11-32](#) for more information.
- Directly-connected and static networks that fall within the defined networks are advertised by the security appliance. Additionally, only interfaces with an IP address that fall within the defined networks participate in the EIGRP routing process.
- If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, configure a network entry on the Setup > Networks tab that covers the network the interface is attached to, and then configure that interface as a passive interface to prevent the interface from sending or receiving EIGRP updates. Interfaces configured as passive do not send or receive EIGRP updates. See [Passive Interfaces, page 11-33](#) for more information.
- Step 5** (Optional) Define route filters on the **Filter Rules** pane. Route filtering provides more control over the routes that are allowed to be sent or received in EIGRP updates. See [Filter Rules, page 11-34](#) for more information.
- Step 6** (Optional) Define route redistribution on the **Redistribution** pane.
- You can redistribute routes discovered by RIP and OSPF into the EIGRP routing process. You can also redistribute static and connected routes into the EIGRP routing process. You do not need to redistribute static or connected routes if they fall within the range of a network configured on the Setup > Networks tab. See [Redistribution, page 11-36](#) for more information.
- Step 7** (Optional) Define static EIGRP neighbors on the **Static Neighbor** pane.
- EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a nonbroadcast network, such as a tunnel, you must manually define that neighbor. When you manually define an EIGRP neighbor, hello packets are sent to that neighbor as unicast messages. See [Static Neighbor, page 11-37](#) for more information.
- Step 8** (Optional) Define summary addresses on the **Summary Address** pane.
- You need to manually define summary addresses if you want to create summary addresses that do not occur at a network number boundary or if you want to use summary addresses on a security appliance with automatic route summarization disabled. See [Summary Address, page 11-38](#) for more information about defining summary addresses. See [Edit EIGRP Process Advanced Properties, page 11-31](#) for information about enabling and disabling automatic route summarization.
- Step 9** (Optional) Define interface-specific EIGRP parameters on the **Interfaces** pane. These parameters include EIGRP message authentication, hold time, hello interval, delay metric, and the use of split-horizon. See [Interface, page 11-35](#) for more information.

- Step 10** (Optional) Control the sending and receiving of default route information in EIGRP updates on the **Default Information** pane. By default, default routes are sent and accepted. See [Default Information, page 11-39](#) for more information.

## Field Information for the EIGRP Panes

This section contains the following topics:

- [Setup, page 11-30](#)
- [Filter Rules, page 11-34](#)
- [Interface, page 11-35](#)
- [Redistribution, page 11-36](#)
- [Static Neighbor, page 11-37](#)
- [Summary Address, page 11-38](#)
- [Default Information, page 11-39](#)

### Setup

Enable and EIGRP process and configure the basic setting for that process on the Setup pane. The Setup pane contains the following tabs:

- [Process Instances, page 11-30](#)
- [Networks, page 11-32](#)
- [Passive Interfaces, page 11-33](#)

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Process Instances

The Process Instances tab lets you enable an EIGRP routing process.

#### Fields

- **Enable this EIGRP Process**—Check this check box to enable an EIGRP routing process. You can only enable one EIGRP routing process on the device. You must enter an autonomous system number for the routing process in the EIGRP Process field before you can save your change.
- **EIGRP Process**—Enter the autonomous system number for the EIGRP process. The autonomous system number can be from 1 to 65535.



- **Advanced**—Click this button to configure the EIGRP process settings, such as the router ID, default metrics, stub routing settings, neighbor change and warning logging, and the administrative distances for the EIGRP routes.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Edit EIGRP Process Advanced Properties

The Edit EIGRP Process Advanced Properties dialog box lets you configure the router ID, default metrics, stub routing settings, neighbor change and warning logging, and the administrative distances of the EIGRP routes for the EIGRP routing process.

### Fields

- **EIGRP**—*Display only*. Displays the autonomous system number for the EIGRP routing process.
- **Router Id**—Enter an IP address to be used as the Router ID for the security appliance in the EIGRP routing process. The router ID is used to identify the originating router for external routes. The IP address does not have to be an address configured on the security appliance, however it must be unique within the routing domain. If not specified, the highest-level IP address on the security appliance is used as the router ID.
- **Auto-Summary**—Check to enable automatic route summarization. Clear to disable automatic route summarization. This setting is enabled by default.
- **Default Metrics**—The default metrics are applied to routes redistributed into the EIGRP routing process. If not specified, you must specify the metrics when you configure the redistribution (see [Redistribution, page 11-36](#)).
  - **Bandwidth**—The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
  - **Loading**—The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
  - **Reliability**—The likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.
  - **Delay**—The route delay in tens of microseconds. Valid values are 1 to 4294967295.
  - **MTU**—The smallest allowed value for the maximum transmission unit, expressed in bytes. Valid values are from 1 to 65535.
- **Stub**—The stub area contains the setting for creating an EIGRP stub routing process. A stub routing process does not maintain a full topology table. At a minimum, stub routing needs a default route to a distribution router, which makes the routing decisions.
  - **Stub Receive only**—Configures the EIGRP stub routing process to receive route information from the neighbor routers but does not send route information to the neighbors. If this option is selected, you cannot select any of the other stub routing options.

- Stub Connected—Advertises connected routes.
- Stub Static—Advertises static routes.
- Stub Redistributed—Advertises redistributed routes.
- Stub Summary—Advertises summary routes.
- Adjacency Changes—Lets you configure the logging of neighbor warning and change messages. Logging for both is enabled by default.
  - Log Neighbor Changes—Check to enable or uncheck to disable the logging of neighbor adjacency changes.
  - Log Neighbor Warnings—Check to enable or uncheck to disable the logging of neighbor adjacency changes. Enter the time interval (in seconds) between repeated neighbor warning messages. Valid values are from 1 to 65535. Repeated warnings are not logged if they occur during this interval.
- Administrative Distance—Lets you configure the administrative distances for internal and external EIGRP routes.
  - Internal Distance—Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values are from 1 to 255. The default value is 90.
  - External Distance—Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values are from 1 to 255. The default value is 170.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Networks

The Network tab lets you specify the networks used by the EIGRP routing process. For an interface to participate in EIGRP routing, it must fall within the range of addresses defined by the network entries. For directly connected and static networks to be advertised, they must also fall within the range of the network entries.

The Network table displays the networks configure for the EIGRP routing process. Each row of the table displays the network address and associated mask configure for the specified EIGRP routing process. To add or change a network, do one of the following:

- To add a new network entry, click **Add**. The Add EIGRP Network dialog box appears.
- To remove a network entry, select the entry in the table and click **Delete**.
- To change a network entry, you must first remove the entry and then add a new one. You cannot edit existing entries.

### Fields

The Add EIGRP Network Entry dialog box fields:

- EIGRP AS—Displays the autonomous system number of the EIGRP routing process.
- IP Address—Enter the IP address of the networks to participate in the EIGRP routing process.
- Network Mask—Select or enter a network mask to apply to the IP address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Passive Interfaces

The Passive Interface tab lets you configure one or more interfaces as passive interfaces. In EIGRP, a passive interface does not send or receive routing updates.

The Passive Interface table lists each interface configured as a passive interface. To configure whether an interface participates in EIGRP routing, do one of the following:

- To specify all interfaces as passive, check the Suppress routing updates on all interfaces check box. Even if an interface is not shown in the Passive Interface table, it will be configured as passive when this check box is selected.
- To add a passive interface entry, click **Add**. The Add EIGRP Passive Interface dialog box appears. You can select the interface you want to make passive in the dialog box.
- To remove a passive interface, select the interface in the table and click **Delete**.

### Fields

Passive Interface pane fields:

- EIGRP Process—The autonomous system number of the EIGRP routing process.
- Suppress routing updates on all interfaces—Check this check box to set all interfaces to passive. Clear this check box to allow all interfaces to send and receive EIGRP updates. Note that the interfaces must also have an associated network entry to participate in EIGRP routing.
- Passive Interfaces table—Displays the interface configured as passive.
  - Interface—Displays the name of the interface.
  - EIGRP Process—Displays the autonomous system number of the EIGRP process.
  - Passive—Displays “true” to indicate that the interface is operating in passive mode.

Add Passive Interface dialog box fields:

- EIGRP AS—The autonomous system number of the EIGRP routing process.
- Interface—Select the interface from the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

- [Configuring EIGRP, page 11-29](#)

**Filter Rules**

The Filter Rules pane displays the route filtering rules configured for the EIGRP routing process. Filter rules let you control which routes are accepted or advertised by the EIGRP routing process.

Each row of the Filter Rule table describes a filter rule for a specific interface or routing protocol. For example, a filter rule with a direction of “in” on the outside interface would apply filtering to any EIGRP updates received on the outside interface. A filter rule with a direction of “out” with OSPF 10 specified as the routing protocol would apply the filter rules to routes redistributed into the EIGRP routing process in outbound EIGRP updates.

To configure filter rules, do one of the following:

- To add a filter rule, click **Add**. The Add Filter Rules dialog box appears.
- To edit a filter rule, select the filter rule in the table and click **Edit**. You can also double-click a filter rule to edit the rule. The Edit Filter Rules dialog box appears.
- To remove a filter rule, select the filter rule in the table and click **Delete**.

**Fields**

The Add/Edit EIGRP Filter Rule Dialog box fields:

- EIGRP—The autonomous system number of the EIGRP routing process.
- Direction—Select “in” for rules that filter routes from incoming EIGRP routing updates. Select “out” to filter routes from EIGRP routing updates sent by the security appliance.
- Routing process—(For outgoing filters only) Specifies the type of route being filtered. You can filter routes redistributed from static, connected, RIP, and OSPF routing processes. Filters that specify a routing process filter those routes from updates sent on all interfaces.
- Id—The OSPF process ID.
- Interface—The interface the filter applies to.
- Add—Opens the Network Rule dialog box.
- Edit—Opens the Network Rule dialog box for the selected network rule.

Add/Edit Network Rule dialog box lets you define an access list for the filter rule. The dialog box contains the following fields:

- Action—Select Permit to allow the specified network to be advertised. Select Deny to prevent the specified network from being advertised.
- IP Address—Type IP address of the network being permitted or denied. To permit or deny all addresses, use the IP address 0.0.0.0 with a network mask of 0.0.0.0.
- Netmask—Specify the network mask applied to the network IP address. You can type a network mask into this field or select one of the common masks from the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### For More Information

- [Configuring EIGRP, page 11-29](#)

## Interface

The Interface pane displays the EIGRP interface configurations. The Interface Parameters table displays all of the interfaces on the security appliance and lets you modify the following settings on a per-interface basis:

- Authentication key and mode.
- The EIGRP hello interval and hold time.
- The interface delay metric used in EIGRP metric calculations.
- The use of split-horizon on the interface.

To configure the EIGRP parameters for an interface, double-click an interface entry or select the entry and click **Edit**. The Edit EIGRP Interface Entry dialog box appears.

### Fields

The Edit EIGRP Interface Entry dialog box fields:

- Interface—*Display only*. Displays the interface being modified.
- AS—The EIGRP autonomous system number.
- Hello Interval—Enter the interval between EIGRP hello packets sent on an interface. Valid values are from 1 to 65535 seconds. The default value is 5 seconds.
- Hold Time—Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds. The default value is 15 seconds.
- Split Horizon—Check this check box to enable split horizon on the interface. Uncheck the check box to disable split horizon. Split horizon is enabled by default.
- Delay—Enter the delay value in this field. The delay time is in tens of microseconds. Valid values are from 1 to 16777215.
- Enable MD5 Authentication—Check this check box to enable MD5 authentication of EIGRP process messages.
  - Key—Key to authenticate EIGRP updates. The key can contain up to 16 characters.
  - Key ID—Key identification value; valid values range from 1 to 255.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

- [Configuring EIGRP, page 11-29](#)

**Redistribution**

The Redistribution pane displays the rules for redistributing routes from other routing protocols into the EIGRP routing process. Each row of the Redistribution pane table contains a route redistribution entry.

To add or modify route redistribution into the EIGRP routing process, do one of the following:

- To add a new redistribution rule, click **Add**. The Add EIGRP Redistribution Entry dialog box opens.
- To edit an existing EIGRP static neighbor, select the address in the table and click **Edit**. You can also double-click an entry in the table to edit that entry. The Edit EIGRP Redistribution Entry dialog box opens.

**Fields**

The Add/Edit EIGRP Redistribution Entry dialog box fields:

- **AS**—Displays the autonomous system number of the EIGRP routing process to which the entry applies.
- **Static**—Redistributes static routes into the EIGRP routing process. Static routes that fall within the scope of a network statement are automatically redistributed into EIGRP; you do not need to define a redistribution rule for them.
- **Connected**—Redistributes connected routes into the EIGRP routing process. Connected routes that fall within the scope of a network statement are automatically redistributed into EIGRP; you do not need to define a redistribution rule for them.
- **RIP**—Redistributes routes discovered by the RIP routing process into EIGRP.
- **Optional Metrics**—Defines the metrics used for the redistributed route. You do not need to define these values if you already defined the default metrics in the **Edit EIGRP Process Advanced Properties** dialog box (see [Edit EIGRP Process Advanced Properties, page 11-31](#) for information about setting the default metrics).
  - **Bandwidth**—EIGRP bandwidth metric in Kilobits per second. Valid values are from 1 to 4294967295.
  - **Delay**—EIGRP delay metric, in 10 microsecond units. Valid values are from 0 to 4294967295.
  - **Reliability**—EIGRP reliability metric. Valid values are from 0 to 255, where 255 indicates 100% reliability.
  - **Loading**—EIGRP effective bandwidth (loading) metric. Valid values are from 1 to 255, where 255 indicates 100% loaded.
  - **MTU**—The MTU of the path. Valid values are from 1 to 65535.
- **Route Map**—To further define which routes are redistributed into the EIGRP routing process, enter the name of a route map.

- Optional OSPF Redistribution—these options let you further specify which OSPF routes are redistributed into the EIGRP routing process.
  - Match Internal—Match routes internal to the specified OSPF process.
  - Match External 1—Match type 1 routes external to the specified OSPF process.
  - Match External 2—Match type 2 routes external to the specified OSPF process.
  - Match NSSA-External 1—Match type 1 routes external to the specified OSPF NSSA.
  - Match NSSA-External 2—Match type 2 routes external to the specified OSPF NSSA.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### For More Information

- [Configuring EIGRP, page 11-29](#)

## Static Neighbor

The Static Neighbor pane displays the statically-defined EIGRP neighbors. An EIGRP neighbor sends EIGRP routing information to and receives EIGRP routing information from the security appliance. Normally, neighbors are dynamically discovered through the neighbor discovery process. However, on point-to-point, non-broadcast networks, you must statically define the neighbors.

Each row of the Static Neighbor table displays the EIGRP autonomous system number for the neighbor, the neighbor IP address, and the interface through which the neighbor is available.

To configure a static neighbor, so one of the following:

- To add a new EIGRP static neighbor, click **Add**. The Add EIGRP Neighbor Entry dialog box opens.
- To edit an existing EIGRP static neighbor, select the address in the table and click **Edit**. You can also double-click an entry in the table to edit that entry. The Edit EIGRP Neighbor Entry dialog box opens.

### Fields

The Add/Edit EIGRP Neighbor Entry dialog box fields:

- EIGRP AS—The autonomous system number for the EIGRP process the neighbor is being configured for.
- Interface Name—Select the interface through which the neighbor is available from the list.
- Neighbor IP Address—Enter the IP address of the neighbor.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

- [Configuring EIGRP, page 11-29](#)

**Summary Address**

The Summary Address pane displays a table of the statically-defined EIGRP summary addresses. By default, EIGRP summarizes subnet routes to the network level. You can create statically-defined EIGRP summary addresses to the subnet level from the Summary Address pane.

To create or modify a summary address, do one of the following:

- To add a new EIGRP summary address, click **Add**. The Add Summary Address dialog box opens.
- To edit an existing EIGRP summary address, select the address in the table and click **Edit**. You can also double-click an entry in the table to edit that entry. The Edit Summary Address dialog box opens.

**Fields**

The Add/Edit EIGRP Summary Address Entry dialog box contains the following fields. These fields are also shown in the Summary Address table.

- EIGRP AS—Select the autonomous system number of the EIGRP routing process the summary address applies to.
- Interface—The interface the summary address is advertised from.
- IP Address—Enter the IP address of the summary route.
- Netmask—Select or enter the network mask to apply to the IP address.
- Administrative Distance—Enter the administrative distance for the route. If left blank, the route has the default administrative distance of 5.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

- [Configuring EIGRP, page 11-29](#)



## Default Information

The Default Information pane displays a table of rules for controlling the sending and receiving of default route information in EIGRP updates. You can have one “in” and one “out” rule for each EIGRP routing process (only one process is currently supported).

By default, default routes are sent and accepted. To restrict or disable the sending and receiving of default route information, perform the following steps:

---

**Step 1** Open the **Configuration > Device Setup > Routing > EIGRP > Default Information** pane.

**Step 2** Do one of the following:

- To create a new entry, click **Add**.
- To edit an entry, double-click the entry in the table or select an entry in the table and click **Edit**.

The Add or Edit Default Information dialog box opens for that entry. The EIGRP autonomous system number is automatically selected in the EIGRP field.

**Step 3** Set the direction for the rule in the **Direction** field:

- in—the rule filters default route information from incoming EIGRP updates.
- out—the rule filters default route information from outgoing EIGRP updates.

You can have one “in” rule and one “out” rule for each EIGRP process.

**Step 4** Add network rules to the network rule table. The network rules define which networks are allowed and which are not when receiving or sending default route information. Repeat the following steps for each network rule you are adding to the default information filter rule.

- a. Click **Add** to add a network rule. Double-click an existing network rule to edit the rule.
- b. In the **Action** field, select **Permit** to allow the network or **Deny** to block the network.
- c. Enter the IP address and network mask of the network being permitted or denied by the rule in the **IP Address** and **Network Mask** fields.

To deny all default route information from being accepted or sent, use 0.0.0.0 as the network address and select 0.0.0.0 as the network mask.

- d. Click **OK** to add the specified network rule to the default information filter rule.

**Step 5** Click **OK** to accept the default information filter rule.

---

### Fields

Add/Edit Default Information dialog box:

- EIGRP—Select the autonomous system number of the EIGRP routing process the default information filter applies to.
- Direction—Select “in” to filter default route information from incoming route updates. Select “out” to filter default route information from outgoing route updates.
- Add—Add a network rule to the default information filter rule.
- Edit—Modify an existing network rule.

Network Rule dialog box. The network rules appear in the Filter Rules column of the Default Information filter rule table.

- Action—Select Permit to allow the specified network to be advertised. Select Deny to prevent the specified network from being advertised.

- **IP Address**—Type IP address of the network being permitted or denied. To permit or deny all addresses, use the IP address 0.0.0.0 with a network mask of 0.0.0.0.
- **Netmask**—Specify the network mask applied to the network IP address. You can type a network mask into this field or select one of the common masks from the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### For More Information

- [Configuring EIGRP, page 11-29](#)

## Static Routes

Multiple context mode does not support dynamic routing, so you must define static routes for any networks to which the security appliance is not directly connected.

In transparent firewall mode, for traffic that originates on the security appliance and is destined for a non-directly connected network, you need to configure either a default route or static routes so the security appliance knows out of which interface to send traffic. Traffic that originates on the security appliance might include communications to a syslog server, Websense or N2H2 server, or AAA server. If you have servers that cannot all be reached through a single default route, then you must configure static routes.

The simplest option is to configure a default route to send all traffic to an upstream router, relying on the router to route the traffic for you. However, in some cases the default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is on the outside interface, the default route cannot direct traffic to any inside networks that are not directly connected to the security appliance.

You can also use static route in conjunction with dynamic routing protocols to provide a floating static route that is used when the dynamically discovered route goes down. If you create a static route with an administrative distance greater than the administrative distance of the dynamic routing protocol, then a route to the specified destination discovered by the routing protocol takes precedence over the static route. The static route is used only if the dynamically discovered route is removed from the routing table.

Static routes remain in the routing table even if the specified gateway becomes unavailable (see [Static Route Tracking, page 11-41](#), for the exception to this). If the specified gateway becomes unavailable, you need to remove the static route from the routing table manually. However, static routes are removed from the routing table if the associated interface on the security appliance goes down. They are reinstated when the interface comes back up.

You can define up to three equal cost routes to the same destination per interface. ECMP is not supported across multiple interfaces. With ECMP, the traffic is not necessarily divided evenly between the routes; traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

The default route identifies the gateway IP address to which the security appliance sends all IP packets for which it does not have a learned or static route. A default route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.

You can define up to three equal cost default route entries per device. Defining more than one equal cost default route entry causes the traffic sent to the default route to be distributed among the specified gateways. When defining more than one default route, you must specify the same interface for each entry.

If you attempt to define more than three equal cost default routes, or if you attempt to define a default route with a different interface than a previously defined default route, you will receive an error message.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all encrypted traffic that arrives on the security appliance and that cannot be routed using learned or static routes is sent to this route. Otherwise, if the traffic is not encrypted, the standard default route entry is used. You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

For more information about viewing and configuring static and default routes with ASDM, see [Field Information for Static Routes, page 11-42](#).

## Static Route Tracking

It is not always possible to use dynamic routing protocols on the security appliance, such as when the security appliance is in multiple context mode or transparent mode. In these cases, you must use static routes.

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway goes down. They are only removed from the routing table if the associated interface on the security appliance goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. This allows you to, for example, define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The security appliance does this by associating a static route with a monitoring target that you define. It monitors the target using ICMP echo requests. If an echo reply is not received within a specified time period, the object is considered down and the associated route is removed from the routing table. A previously configured backup route is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that responds to ICMP echo requests. Consider choosing:

- the ISP gateway (for dual ISP support) address
- the next hop gateway address (if you are concerned about the availability of the gateway)
- a server, such as a AAA server, that the security appliance needs to communicate with
- a persistent network object on the destination network (a desktop or notebook computer that may be shut down at night is not a good choice)

For more information about configuring static route tracking, see [Configuring Static Route Tracking, page 11-42](#). To monitor the static route tracking process, see [interface connection, page 41-9](#).

## Configuring Static Route Tracking

This procedure provides an overview of configuring static route tracking. For specific information about the various fields used to configure this feature, see [Field Information for Static Routes, page 11-42](#).

To configure tracking for a static route, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose a target of interest. Make sure the target responds to echo requests.                                                                                                                                                                                                                                        |
| <b>Step 2</b> | Open the Static Routes page. Go to <b>Configuration &gt; Routing &gt; Static Routes</b> .                                                                                                                                                                                                                           |
| <b>Step 3</b> | Click <b>Add</b> to configure a static route that is to be used based on the availability of your selected target of interest. You must enter the Interface, IP Address, Mask, Gateway, and Metric for this route. See <a href="#">Add/Edit Static Route, page 11-43</a> , for more information about these fields. |
| <b>Step 4</b> | Choose <b>Tracked</b> in the Options area for this route.                                                                                                                                                                                                                                                           |
| <b>Step 5</b> | Configure the tracking properties. You must enter a unique Track ID, a unique SLA ID, and the IP address of your target of interest. See <a href="#">Add/Edit Static Route, page 11-43</a> , for more information about these fields.                                                                               |
| <b>Step 6</b> | (Optional) To configure the monitoring properties, click <b>Monitoring Options</b> in the Add Static Route dialog box. See <a href="#">Route Monitoring Options, page 11-44</a> , for more information about the monitoring properties.                                                                             |
| <b>Step 7</b> | Click <b>OK</b> to save your changes.<br><br>The monitoring process begins as soon as you save the tracked route.                                                                                                                                                                                                   |
| <b>Step 8</b> | Create a secondary route. The secondary route is a static route to the same destination as the tracked route, but through a different interface or gateway. You must assign this route a higher administrative distance (metric) than your tracked route.                                                           |
- 

## Field Information for Static Routes

For information about a specific pane, see the following topics:

- [Static Routes, page 11-42](#)
- [Add/Edit Static Route, page 11-43](#)
- [Route Monitoring Options, page 11-44](#)

## Static Routes

The Static Route pane lets you create static routes that will access networks connected to a router on any interface. To enter a default route, set the IP address and mask to 0.0.0.0, or the shortened form of 0.

If an IP address from one security appliance interface is used as the gateway IP address, the security appliance will ARP the designated IP address in the packet instead of ARPing the gateway IP address.

Leave the Metric at the default of 1 unless you are sure of the number of hops to the gateway router.

### Fields

The Static Route pane shows the Static Route table:

- **Interface**—(*Display only*) Lists the internal or external network interface name enabled in Interfaces.
- **IP Address**—(*Display only*) Lists the internal or external network IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** IP address can be abbreviated as **0**.
- **Netmask**—(*Display only*) Lists the network mask address that applies to the IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** netmask can be abbreviated as **0**.
- **Gateway IP**—(*Display only*) Lists the IP address of the gateway router, which is the next hop address for this route.
- **Metric**—(*Display only*) Lists the administrative distance of the route. The default is 1 if a metric is not specified.
- **Options**—(*Display only*) Displays any options specified for the static route.
  - **None**—No options are specified for the static route.
  - **Tunneled**—Specifies route as the default tunnel gateway for VPN traffic. Used only for default route. You can only configure one tunneled route per device. The tunneled option is not supported under transparent mode.
  - **Tracked**—Specifies that the route is tracked. The tracking object ID and the address of the tracking target are also displayed. The tracked option is only supported in single, routed mode.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Static Route

Use the Add/Edit Static Route dialog box to configure the static route properties. This dialog box is available from both the Static Routes screen in the Startup Wizard and the Configuration > Routing > Static Route pane.

### Fields

- **Interface Name**—Select the egress interface for the route.
- **IP Address**—Specifies the internal or external network IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** IP address can be abbreviated as **0**.
- **Mask**—Specifies the network mask address that applies to the IP address. Use **0.0.0.0** to specify a default route. The **0.0.0.0** netmask can be abbreviated as **0**.
- **Gateway IP**—Specifies the IP address of the gateway router, which is the next hop address for this router.
- **Metric**—Lets you specify the administrative distance of the route. The default is **1** if a metric is not specified.

The following options are available for static routes. You can select only one of these options for a static route. By default, no option (None) is selected.

- None—No options are specified for the static route.
- Tunneled—Used only for default route. Only one default tunneled gateway is allowed per security appliance. Tunneled option is not supported under transparent mode.
- Tracked—Select this option to specify that the route is tracked. Specifying this option starts the route tracking process.
  - Track ID—A unique identifier for the route tracking process.
  - Track IP Address/DNS Name—Enter the IP address or hostname of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.
  - SLA ID—A unique identifier for the SLA monitoring process.
  - Monitor Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Route Monitoring Options

Use the Route Monitoring Options dialog box to change the tracking object monitoring properties.

### Fields

- Frequency—Enter how often, in seconds, the security appliance should test for the presence of the tracking target. The default value is 60 seconds. Valid values are from 1 to 604800 seconds.
- Threshold—Enter the amount of time, in milliseconds, that indicates an over-threshold event. This value cannot be more than the timeout value.
- Timeout—Enter the amount of time, in milliseconds, the route monitoring operation should wait for a response from the request packets. The default value is 5000 milliseconds. Valid values are from 0 to 604800000 milliseconds.
- Data Size—Enter the size of data payload to use in the echo request packets. The default value is 28. Valid values are from 0 to 16384.



#### Note

This setting specifies the size of the payload only; it does not specify the size of the entire packet.

- ToS—Enter a value for the type of service byte in the IP header of the echo request. The default value is 0. Valid values are from 0 to 255.
- Number of Packets—The number of echo requests to send for each test. The default value is 1. Valid values are from 1 to 100.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## ASR Group

Use the ASR Group screen to assign asynchronous routing group ID numbers to interfaces.

In some situations, return traffic for a session may be routed through a different interface than it originated from. In failover configurations, return traffic for a connection that originated on one unit may return through the peer unit. This most commonly occurs when two interfaces on a single security appliance, or two security appliances in a failover pair, are connected to different service providers and the outbound connection does not use a NAT address. By default, the security appliance drops the return traffic because there is no connection information for the traffic.

You can prevent the return traffic from being dropped using an ASR Group on interfaces where this is likely to occur. When an interface configured with an ASR Group receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same group.

If it does not find a match, the packet is dropped. If it finds a match, then one of the following actions occurs:

- If the incoming traffic originated on a peer unit in a failover configuration, some or all of the layer 2 header is rewritten and the packet is redirected to the other unit. This redirection continues as long as the session is active.
- If the incoming traffic originated on a different interface on the same unit, some or all of the layer 2 header is rewritten and the packet is reinjected into the stream.

### Prerequisites

You must enable Stateful Failover for session information to be passed from the standby failover group to the active failover group.

### Fields

The **ASR Group** table displays the following information for each interface on the security appliance:

- **Interface**—Displays the name of the interface on the security appliance.
- **ASR Group ID**—Displays the number of the ASR Group the interface belongs to. If the interface has not been assigned an ASR Group number, this column displays "-- None --". Valid values are from 1 to 32.

To assign an ASR Group number to an interface, click the **ASR Group ID** cell in the row of the desired interface. A list of valid ASR Group number appears. Select the desired ASR Group number from the list. You can assign a maximum of 8 interfaces to a single ASR Group. If other contexts have interfaces assigned to an ASR Group, those interface count against the total of 8, even for the context currently being configured.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | •        | —      |

## Proxy ARPs

In rare circumstances, you might want to disable proxy ARP for global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking “Who is this IP address?” The device owning the IP address replies, “I own that IP address; here is my MAC address.”

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The security appliance uses proxy ARP when you configure NAT and specify a global address that is on the same network as the security appliance interface. The only way traffic can reach the hosts is if the security appliance uses proxy ARP to claim that the security appliance MAC address is assigned to destination global addresses.

**Fields**

- Interface—Lists the interface names.
- Proxy ARP Enabled—Shows whether proxy ARP is enabled or disabled for NAT global addresses, Yes or No.
- Enable—Enables proxy ARP for the selected interface. By default, proxy ARP is enabled for all interfaces.
- Disable—Disables proxy ARP for the selected interface.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |





# CHAPTER 12

## Configuring Multicast Routing

Multicast routing is supported in single, routed mode only. This section contains the following topics:

- [Multicast, page 12-1](#)—enable or disable multicast routing on the security appliance.
- [IGMP, page 12-2](#)—configure IGMP on the security appliance.
- [Multicast Route, page 12-7](#)—define static multicast routes.
- [MBoundary, page 12-9](#)—configure boundaries for administratively-scoped multicast addresses.
- [MForwarding, page 12-11](#)—enable or disable multicast forwarding on a per-interface basis.
- [PIM, page 12-11](#)—configure PIM on the security appliance.

## Multicast

The Multicast pane lets you enable multicast routing on the security appliance.

Enabling multicast routing enables IGMP and PIM on all interfaces by default. IGMP is used to learn whether members of a group are present on directly attached subnets. Hosts join multicast groups by sending IGMP report messages. PIM is used to maintain forwarding tables to forward multicast datagrams.



**Note**

Only the UDP transport layer is supported for multicast routing.

### Fields

**Enable Multicast Routing**—Check this check box to enable IP multicast routing on the security appliance. Uncheck this check box to disable IP multicast routing. By default, multicast is disabled. Enabling multicast enables multicast on all interfaces. You can disable multicast on a per-interface basis.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**[Configuring Multicast Routing, page 12-1](#)[IGMP, page 12-2](#)[Multicast Route, page 12-7](#)[MBoundary, page 12-9](#)[MForwarding, page 12-11](#)[PIM, page 12-11](#)

## IGMP

IP hosts use IGMP to report their group memberships to directly connected multicast routers. IGMP uses group address (Class D IP addresses). Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is never assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

For more information about configuring IGMP on the security appliance, see the following:

- [Access Group](#)
- [Join Group](#)
- [Protocol](#)
- [Static Group](#)

## Access Group

Access groups control the multicast groups that are allowed on an interface.

**Fields**

- Access Groups—Displays the access groups defined for each interface.

The table entries are processed from the top down. Place more specific entries near the top of the table and more generic entries further down. For example, place an access group entry that permits a specific multicast group near the top of the table and an access group entry below that denies a range of multicast groups, including the group in the permit rule. The group is permitted because the permit rule is enforced before the deny rule.

Double-clicking an entry in the table opens the [Add/Edit Access Group](#) dialog box for the selected entry.

- Interface—Displays the interface the access group is associated with.
- Action—Displays “Permit” if the multicast group address is permitted by the access rule. Displays “Deny” if the multicast group address is denied by the access rule.
- Multicast Group Address—Displays the multicast group address that the access rule applies to.
- Netmask—Displays the network mask for the multicast group address.
- Insert Before—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry before the selected entry in the table.
- Insert After—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry after the selected entry in the table.

- **Add**—Opens the [Add/Edit Access Group](#) dialog box. Use this button to add a new access group entry at the bottom of the table.
- **Edit**—Opens the [Add/Edit Access Group](#) dialog box. Use this button to change the information for the selected access group entry.
- **Delete**—Removes the selected access group entry from the table.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Access Group

The Add Access Group dialog box lets you add a new access group to the Access Group Table. The Edit Access Group dialog box lets you change information for an existing access group entry. Some fields may be locked when editing existing entries.

#### Fields

- **Interface**—Choose the interface the access group is associated with. You cannot change the associated interface when you are editing an existing access group.
- **Action**—Choose “permit” to allow the multicast group on the selected interface. Choose “deny” to filter the multicast group from the selected interface.
- **Multicast Group Address**—Enter the address of the multicast group the access group applies to.
- **Netmask**—Enter the network mask for the multicast group address or choose one of the common network masks from the list.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Join Group

You can configure the security appliance to be a member of a multicast group. The Join Group pane displays the multicast groups the security appliance is a member of.

**Note**

If you simply want to forward multicast packets for a specific group to an interface without the security appliance accepting those packets as part of the group, see [Static Group](#).

**Fields**

- **Join Group**—Displays the multicast group membership for each interface.
  - **Interface**—Displays the name of the security appliance interface.
  - **Multicast Group Address**—Displays the address of a multicast group that the interface belongs to.
- **Add**—Opens the [Add/Edit IGMP Join Group](#) dialog box. Use this button to add a new multicast group membership to an interface.
- **Edit**—Opens the [Add/Edit IGMP Join Group](#) dialog box. Use this button to edit an existing multicast group membership entry.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit IGMP Join Group

Use the Add IGMP Join Group dialog box to configure an interface to be a member of a multicast group. Use the Edit IGMP Join Group dialog box to change existing membership information.

**Fields**

- **Interface**—Choose the name of the security appliance interface that you are configuring multicast group membership for. If you are editing an existing entry, you cannot change this value.
- **Multicast Group Address**—Enter the address of a multicast group in this field. The group address must be from 224.0.0.0 to 239.255.255.255.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Protocol

The Protocol pane displays the IGMP parameters for each interface on the security appliance.

### Fields

- Protocol—Displays the IGMP parameters set on each interface. Double-clicking a row in the table opens the [Configure IGMP Parameters](#) dialog box for the selected interface.
  - Interface—Displays the name of the interface.
  - Enabled—Displays “Yes” if IGMP is enabled on the interface. Displays “No” if IGMP is disabled on the interface.
  - Version—Displays the version of IGMP enabled on the interface.
  - Query Interval—Displays the interval, in seconds, at which the designated router sends IGMP host-query messages.
  - Query Timeout—Displays the period of time before which the security appliance takes over as the querier for the interface after the previous querier has stopped doing so.
  - Response Time—Displays the maximum response time, in seconds, advertised in IGMP queries. Changes to this setting are valid only for IGMP Version 2.
  - Group Limit—Displays the maximum number of groups permitted on an interface.
  - Forward Interface—Displays the name of the interface that the selected interface forwards IGMP host reports to.
- Edit—Opens the [Configure IGMP Parameters](#) dialog box for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configure IGMP Parameters

The Configure IGMP Parameters dialog box lets you disable IGMP and change IGMP parameters on the selected interface.

### Fields

- Interface—Displays the name of the interface being configured. You cannot change the information displayed in this field.
- Enable IGMP—Check this check box to enable IGMP on the interface. Uncheck the check box to disable IGMP on the interface. If you enabled multicast routing on the security appliance, then IGMP is enabled by default.
- Version—Choose the version of IGMP to enable on the interface. Choose 1 to enable IGMP Version 1, or 2 to enable IGMP Version 2. Some features require IGMP Version 2. By default, the security appliance uses IGMP Version 2.

- **Query Interval**—Enter the interval, in seconds, at which the designated router sends IGMP host-query messages. Valid values range from 1 to 3600 seconds. The default value is 125 seconds.
- **Query Timeout**—Enter the period of time, in seconds, before which the security appliance takes over as the querier for the interface after the previous querier has stopped doing so. Valid values range from 60 to 300 seconds. The default value is 255 seconds.
- **Response Time**—Enter the maximum response time, in seconds, advertised in IGMP queries. If the security appliance does not receive any host reports within the designated response time, the IGMP group is pruned. Decreasing this value lets the security appliance prune groups faster. Valid values range from 1 to 12 seconds. The default value is 10 seconds. Changing this value is only valid only for IGMP Version 2.
- **Group Limit**—Enter the maximum number of host that can join on an interface. Valid values range from 1 to 500. The default value is 500.
- **Forward Interface**—Choose the name of an interface to forward IGMP host reports to. Choose “None” to disable host report forwarding. By default, host reports are not forwarded.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Static Group

Sometimes, hosts on a network may have a configuration that prevents them from answering IGMP queries. However, you still want multicast traffic to be forwarded to that network segment. There are two methods to pull multicast traffic down to a network segment:

- Use the [Join Group](#) pane to configure the interface as a member of the multicast group. With this method, the security appliance accepts the multicast packets in addition to forwarding them to the specified interface.
- Use the Static Group pane configure the security appliance to be a statically connected member of a group. With this method, the security appliance does not accept the packets itself, but only forwards them. Therefore, this method allows fast switching. The outgoing interface appears in the IGMP cache, but itself is not a member of the multicast group.

### Fields

- **Static Group**—Displays the statically assigned multicast groups for each interface.
  - **Interface**—Displays the name of the security appliance interface.
  - **Multicast Group Address**—Displays the address of a multicast group assigned to the interface.
- **Add**—Opens the [Add/Edit IGMP Static Group](#) dialog box. Use this button to assign a new static group to an interface.
- **Edit**—Opens the [Add/Edit IGMP Static Group](#) dialog box. Use this button to edit an existing static group membership.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**Add/Edit IGMP Static Group**

Use the Add IGMP Static Group dialog box to statically assign a multicast group to an interface. Use the Edit IGMP Static Group dialog box to change existing static group assignments.

**Fields**

- **Interface**—Choose the name of the security appliance interface that you are configuring a multicast group for. If you are editing an existing entry, you cannot change this value.
- **Multicast Group Address**—Enter the address of a multicast group in this field. The group address must be from 224.0.0.0 to 239.255.255.255.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**Multicast Route**

Defining static multicast routes lets you separate multicast traffic from unicast traffic. For example, when a path between a source and destination does not support multicast routing, the solution is to configure two multicast devices with a GRE tunnel between them and to send the multicast packets over the tunnel.

Static multicast routes are local to the security appliance and are not advertised or redistributed.

**Fields**

- **Multicast Route**—Displays the statically-defined multicast routes on the security appliance. Double-clicking an entry in the table opens the [Add/Edit Multicast Route](#) dialog box for that entry.
  - **Source Address**—Displays the IP address and mask, in CIDR notation, of the multicast source.
  - **Source Interface**—Displays the incoming interface for the multicast route.
  - **Destination Interface**—Displays the outgoing interface for the multicast route.
  - **Admin Distance**—Displays the administrative distance of the static multicast route.
- **Add**—Opens the [Add/Edit Multicast Route](#) dialog box. Use this button to add a new static route.

- **Edit**—Opens the [Add/Edit Multicast Route](#) dialog box. Use this button to change the selected static multicast route.
- **Delete**—Use this button to remove the selected static route.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Multicast Route

Use the Add Multicast Route dialog box to add a new static multicast route to the security appliance. Use the Edit Multicast Route dialog box to change an existing static multicast route.

### Fields

- **Source Address**—Enter the IP address of the multicast source. You cannot change this value when editing an exiting static multicast route.
- **Source Mask**—Enter the network mask for the IP address of the multicast source or chose a common mask from the list. You cannot change this value when editing an exiting static multicast route.
- **Source Interface**—Choose the incoming interface for the multicast route.
- **Destination Interface**—(Optional) Choose the outgoing interface for the multicast route. If you specify the destination interface, the route is forwarded through the selected interface. If you do not choose a destination interface, then RPF is used to forward the route. You can specify the interface, or the RPF neighbor, but not both at the same time.
- **Admin Distance**—Enter the administrative distance of the static multicast route. If the static multicast route has the same administrative distance as the unicast route, then the static multicast route takes precedence.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |



# MBoundary

The MBoundary pane lets you configure a multicast boundary for administratively-scoped multicast addresses. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains. When a multicast boundary is defined on an interface, only the multicast traffic permitted by the filter ACL passes through the interface.

## Fields

The Multicast Boundary table contains the following information. Double-click a table entry to edit the multicast boundary filter settings.

- **Interface**—Lists the interfaces on the device.
- **Boundary Filter**—Lists the boundary filter entries for the specified interface. If a multicast boundary has not been defined for an interface, then this column displays “No Boundary Filters Configured” for the interface.
- **AutoFilter**—Shows if Auto-RP messages are denied by the boundary ACL. If the AutoFilter is enabled, the ACL also restricts the flow of Auto-RP messages. If the AutoFilter is disabled, all Auto-RP messages are passed by the interface. This setting is disabled by default.

You can perform the following actions on the entries of the Boundary table:

- **Edit**—Opens the Edit Boundary Filter dialog box.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit Boundary Filter

The Edit Boundary Filter dialog box displays the multicast boundary filter ACL. You can add and remove boundary filter ACL entries using this dialog box.

When the boundary filter configuration is applied to the security appliance, the ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*.

## Fields

- **Interface**—Displays the interface for which you are configuring the multicast boundary filter ACL.
- **Remove any Auto-RP group range**—Check this check box to filter Auto-RP messages from sources denied by the boundary ACL. If not checked, all Auto-RP messages are passed.

The Boundary Filter table contains the following information:

- **Action**—The action for the filter entry. Permit allows the specified traffic to pass. Deny prevents the specified traffic from passing through the interface. When a multicast boundary filter is configured on an interface, multicast traffic is denied by default.
- **Network Address**—The multicast group address of the group being permitted or denied.
- **Netmask**—The network mask applied to the multicast group address.

You can perform the following actions on the Boundary Filter table:

- **Insert**—Inserts a neighbor filter entry before the selected entry.
- **Add**—Adds a neighbor filter entry after the selected entry.
- **Edit**—Edits the selected boundary filter.
- **Delete**—Removes the selected neighbor filter entry.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit/Insert Neighbor Filter Entry

The Add/Edit/Insert Neighbor Filter Entry dialog box lets you create the ACL entries for the multicast boundary ACL.

### Fields

- **Action**—Select Permit or Deny for the neighbor filter ACL entry. Selecting Permit allows the multicast group advertisements through the interface. Selecting Deny prevents the specified multicast group advertisements from passing through the interface. When a multicast boundary is configured on an interface, all multicast traffic is prevented from passing through the interface unless permitted with a neighbor filter entry.
- **Multicast Group Address**—Enter the address of the multicast group being permitted or denied. Valid group addresses are from 224.0.0.0 to 239.255.255.255.
- **Netmask**—Type or select the netmask for the multicast group address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

# MForwarding

The MForwarding pane lets you disable and reenable multicast forwarding on a per interface basis. By default, multicast forwarding is enabled on all interfaces.

When multicast forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when multicast forwarding is disabled.

## Fields

- The Multicast Forwarding table displays the following information:
  - Interface—Displays the interfaces configured on the security appliance. Click an interface name to select the interface. Double-click an interface name to toggle the Multicast Forwarding Enabled status for the interface.
  - Multicast Forwarding Enabled—Displays Yes if multicast forwarding is enabled on the specified interface. Displays No if multicast forwarding is disabled on the specified interface. Double-click this entry to toggle Yes/No for the selected interface.
- Enable—Enables multicast forwarding on the selected interface.
- Disable—Disables multicast forwarding on the selected interface.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## For More Information

- [Configuring Multicast Routing, page 12-1](#)

# PIM

Routers use PIM to maintaining forwarding tables for forwarding multicast datagrams.

When you enable multicast routing on the security appliance, PIM is enabled on all interfaces by default. You can disable PIM on a per-interface basis.

For more information about configuring PIM, see the following:

- [Protocol](#)
- [Neighbor Filter, page 12-13](#)
- [Bidirectional Neighbor Filter, page 12-14](#)
- [Rendezvous Points](#)
- [Route Tree](#)
- [Request Filter](#)

## Protocol

The Protocol pane displays the interface-specific PIM properties.

### Fields

- **Protocol**—Displays the PIM settings for each interface. Double-clicking an entry in the table opens the [Edit PIM Protocol](#) dialog box for that entry.
  - **Interface**—Displays the name of the security appliance interfaces.
  - **PIM Enabled**—Displays “Yes” if PIM is enabled on the interface, “No” if PIM is not enabled.
  - **DR Priority**—Displays the interface priority.
  - **Hello Interval**—Displays the frequency, in seconds, at which the interface sends PIM hello messages.
  - **Join-Prune Interval**—Displays the frequency, in seconds, at which the interface sends PIM join and prune advertisements.
- **Edit**—Opens the [Edit PIM Protocol](#) dialog box for the selected entry.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit PIM Protocol

The Edit PIM Protocol dialog box lets you change the PIM properties for the selected interface.

### Fields

- **Interface**—*Display only*. Displays the name of the selected interface. You cannot edit this value.
- **PIM Enabled**—Check this check box to enable PIM on the selected interface. Uncheck this check box to disable PIM on the selected interface.
- **DR Priority**—Sets the designated router priority for the selected interface. The router with the highest DR priority on subnet becomes the designated router. Valid values range from 0 to 4294967294. The default DR priority is 1. Setting this value to 0 makes the security appliance interface ineligible to become the default router.
- **Hello Interval**—Enter the frequency, in seconds, at which the interface sends PIM hello messages. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.
- **Join-Prune Interval**—Enter the frequency, in seconds, at which the interface sends PIM join and prune advertisements. Valid values range from 10 to 600 seconds. The default value is 60 seconds.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Neighbor Filter

The Neighbor Filter pane displays the PIM neighbor filters, if any, that are configured on the security appliance. A PIM neighbor filter is an ACL that defines the neighbor devices that can participate in PIM. If a neighbor filter is not configured for an interface, then there are no restrictions. If a PIM neighbor filter is configured, only those neighbors permitted by the filter list can participate in PIM with the security appliance.

When a PIM neighbor filter configuration is applied to the security appliance, an ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*. This ACL defines which devices can become PIM neighbors of the security appliance.

### Fields

The PIM Neighbor Filter table displays the following information. Double-clicking an entry in the table opens the Edit Neighbor Filter Entry dialog box for the selected entry.

- **Interface**—Displays the name of the interface the PIM neighbor filter entry applies to.
- **Action**—Display “permit” if the specified neighbors are allowed to participate in PIM. Displays “deny” if the specified neighbors are prevented from participating in PIM.
- **Network Address**—The network address of the neighbor or neighbors being permitted or denied.
- **Netmask**—The network mask to use with the Network Address.

You can perform the following actions:

- **Insert**—Click to insert a neighbor filter entry before the selected entry.
- **Add**—Click to add a neighbor filter entry after the selected entry.
- **Edit**—Click to edit the selected neighbor filter entry.
- **Delete**—Click to remove the selected neighbor filter entry.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### For More Information

[Add/Edit/Insert Neighbor Filter Entry, page 12-14](#)

## Add/Edit/Insert Neighbor Filter Entry

The Add/Edit/Insert Neighbor Filter Entry lets you create ACL entries for the PIM neighbor filter ACL.

### Fields

- **Interface**—Select the name of the interface the PIM neighbor filter entry applies to from the list.
- **Action**—Select “permit” to allow the specified neighbors to participate in PIM. Select “deny” to prevent the specified neighbors from participating in PIM.
- **Network Address**—The network address of the neighbor or neighbors being permitted or denied.
- **Netmask**—The network mask to use with the Network Address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Bidirectional Neighbor Filter

The Bidirectional Neighbor Filter pane shows the PIM bidirectional neighbor filters, if any, that are configured on the security appliance. A PIM bidirectional neighbor filter is an ACL that defines the neighbor devices that can participate in the DF election. If a PIM bidirectional neighbor filter is not configured for an interface, then there are no restrictions. If a PIM bidirectional neighbor filter is configured, only those neighbors permitted by the ACL can participate in DF election process.

When a PIM bidirectional neighbor filter configuration is applied to the security appliance, an ACL appears in the running configuration with the name *interface-name\_multicast*, where the *interface-name* is the name of the interface the multicast boundary filter is applied to. If an ACL with that name already exists, a number is appended to the name, for example *inside\_multicast\_1*. This ACL defines which devices can become PIM neighbors of the security appliance.

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for *bidir* to elect a DF.

The PIM bidirectional neighbor filters enable the transition from a sparse-mode-only network to a *bidir* network by letting you specify the routers that should participate in DF election while still allowing all routers to participate in the sparse-mode domain. The *bidir*-enabled routers can elect a DF from among themselves, even when there are non-*bidir* routers on the segment. Multicast boundaries on the non-*bidir* routers prevent PIM messages and data from the *bidir* groups from leaking in or out of the *bidir* subset cloud.

When a PIM bidirectional neighbor filter is enabled, the routers that are permitted by the ACL are considered to be *bidir*-capable. Therefore:

- If a permitted neighbor does not support *bidir*, the DF election does not occur.
- If a denied neighbor supports *bidir*, then DF election does not occur.
- If a denied neighbor does not support *bidir*, the DF election can occur.

### Fields

The PIM Bidirectional Neighbor Filter table contains the following entries. Double-click an entry to open the Edit Bidirectional Neighbor Filter Entry dialog box for that entry.

- **Interface**—Displays the interface the bidirectional neighbor filter applies to.
- **Action**—Displays “permit” if the bidirectional neighbor filter entry allows participation in the DF election process. Display “deny” if the entry prevents the specified addresses from participating in the DF election process.
- **Network Address**—The address being permitted or denied.
- **Netmask**—The network mask to apply to the Network Address.

You can perform the following actions:

- **Insert**—Click to insert a bidirectional neighbor filter entry before the selected entry.
- **Add**—Click to add a bidirectional neighbor filter entry after the selected entry.
- **Edit**—Click to edit the selected bidirectional neighbor filter entry.
- **Delete**—Click to remove the selected bidirectional neighbor filter entry.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### For More Information

[Add/Edit/Insert Bidirectional Neighbor Filter Entry, page 12-15](#)

## Add/Edit/Insert Bidirectional Neighbor Filter Entry

The Add/Edit/Insert Bidirectional Neighbor Filter Entry dialog box lets you create ACL entries for the PIM bidirectional neighbor filter ACL.

### Fields

- **Interface**—Select the interface for which you are configuring the PIM bidirectional neighbor filter ACL entry.
- **Action**—Select permit to allow the specified devices to participate in the DF election. Select deny to prevent the specified devices from participating in the DF election.
- **Network Address**—The network address of the neighbor or neighbors being permitted or denied.
- **Netmask**—The network mask to use with the Network Address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Rendezvous Points

When you configure PIM, you must choose one or more routers to operate as the RP. An RP is a single, common root of a shared distribution tree and is statically configured on each router. First hop routers use the RP to send register packets on behalf of the source multicast hosts.

You can configure a single RP to serve more than one group. If a specific group is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

You can configure more than one RP, but you cannot have more than one entry with the same RP.

### Fields

- Generate IOS compatible register messages—Check this check box if your RP is a Cisco IOS router. The security appliance software accepts register messages with the checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS software method—accepting register messages with the checksum on the entire PIM message for all PIM message types.
- Rendezvous Points—Displays the RPs configured on the security appliance.
  - Rendezvous Point—Displays the IP address of the RP.
  - Multicast Groups—Displays the multicast groups associated with the RP. Displays “--All Groups--” if the RP is associated with all multicast groups on the interface.
  - Bi-directional—Displays “Yes” if the specified multicast groups are to operate in bidirectional mode. Displays “No” if the specified groups are to operate in sparse mode.
- Add—Opens the [Add/Edit Rendezvous Point](#) dialog box. Use this button to add a new RP entry.
- Edit—Opens the [Add/Edit Rendezvous Point](#) dialog box. Use this button to change an existing RP entry.
- Delete—Removes the selected RP entry from the Rendezvous Point table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Rendezvous Point

The Add Rendezvous Point dialog box lets you add a new entry to the Rendezvous Point table. The Edit Rendezvous Point dialog box lets you change an existing RP entry.



### Restrictions

- You cannot use the same RP address twice.
- You cannot specify All Groups for more than one RP.

### Fields

- Rendezvous Point IP Address—Enter the IP address of the RP. This is a unicast address. When editing an existing RP entry, you cannot change this value.
- Use bi-directional forwarding—Check this check box if you want the specified multicast groups to operation in bidirectional mode. In bidirectional mode, if the security appliance receives a multicast packet and has no directly connected members or PIM neighbors present, it sends a Prune message back to the source. Uncheck this check box if you want the specified multicast groups to operate in sparse mode.



**Note** The security appliance always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

- Use this RP for All Multicast Groups—Choose this option to use the specified RP for all multicast groups on the interface.
- Use this RP for the Multicast Groups as specified below—Choose this option to designate the multicast groups to use with specified RP.
- Multicast Groups—Displays the multicast groups associated with the specified RP.

The table entries are processed from the top down. You can create an RP entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the [Multicast Group](#) dialog box for the selected entry.

- Action—Displays “Permit” if the multicast group is included or “deny” if the multicast group is excluded.
- Multicast Group Address—Displays the address of the multicast group.
- Netmask—Displays the network mask of the multicast group address.
- Insert Before—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- Insert After—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- Add—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry at the bottom of the table.
- Edit—Opens the [Multicast Group](#) dialog box. Use this button to change the information for the selected multicast group entry.
- Delete—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Multicast Group

Multicast groups are lists of access rules that define which multicast addresses are part of the group. A multicast group can contain a single multicast address or a range of multicast addresses. Use the Add Multicast Group dialog box to create a new multicast group rule. Use the Edit Multicast Group dialog box to modify an existing multicast group rule.

### Fields

- Action—Choose “Permit” to create a group rule that allows the specified multicast addresses; choose “Deny” to create a group rule that filters the specified multicast addresses.
- Multicast Group Address—Enter the multicast address associated with the group.
- Netmask—Enter or choose the network mask for the multicast group address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Request Filter

When the security appliance is acting as an RP, you can restrict specific multicast sources from registering with it. This prevents unauthorized sources from registering with the RP. The Request Filter pane lets you define the multicast sources from which the security appliance will accept PIM register messages.

### Fields

- Multicast Groups—Displays the request filter access rules.

The table entries are processed from the top down. You can create an entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the [Request Filter Entry](#) dialog box for the selected entry.

- Action—Displays “Permit” if the multicast source is allowed to register or “deny” if the multicast source is excluded.
- Source—Displays the address of the source of the register message.

- Destination—Displays the multicast destination address.
- Insert Before—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- Insert After—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- Add—Opens the [Request Filter Entry](#) dialog box. Use this button to add a new multicast group entry at the bottom of the table.
- Edit—Opens the [Request Filter Entry](#) dialog box. Use this button to change the information for the selected multicast group entry.
- Delete—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Request Filter Entry

The Request Filter Entry dialog box lets you define the multicast sources that are allowed to register with the security appliance when the security appliance acts as an RP. You create the filter rules based on the source IP address and the destination multicast address.

### Fields

- Action—Choose “Permit” to create a rule that allows the specified source of the specified multicast traffic to register with the security appliance; choose “Deny” to create a rule that prevents the specified source of the specified multicast traffic from registering with the security appliance.
- Source IP Address—Enter the IP address for the source of the register message.
- Source Netmask—Enter or choose the network mask for the source of the register message.
- Destination IP Address—Enter the multicast destination address.
- Destination Netmask—Enter or choose the network mask for the multicast destination address.

### Modes

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Route Tree

By default, PIM leaf routers join the shortest-path tree immediately after the first packet arrives from a new source. This reduces delay, but requires more memory than shared tree.

You can configure whether the security appliance should join shortest-path tree or use shared tree, either for all multicast groups or only for specific multicast addresses.

### Fields

- **Use Shortest Path Tree for All Groups**—Choose this option to use shortest-path tree for all multicast groups.
- **Use Shared Tree for All Groups**—Choose this option to use shared tree for all multicast groups.
- **Use Shared Tree for the Groups specified below**—Choose this option to use shared tree for the groups specified in the Multicast Groups table. Shortest-path tree is used for any group not specified in the Multicast Groups table.
- **Multicast Groups**—Displays the multicast groups to use Shared Tree with.

The table entries are processed from the top down. You can create an entry that includes a range of multicast groups but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.

Double-click an entry to open the [Multicast Group](#) dialog box for the selected entry.

- **Action**—Displays “Permit” if the multicast group is included or “deny” if the multicast group is excluded.
- **Multicast Group Address**—Displays the address of the multicast group.
- **Netmask**—Displays the network mask of the multicast group address.
- **Insert Before**—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry before the selected entry in the table.
- **Insert After**—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry after the selected entry in the table.
- **Add**—Opens the [Multicast Group](#) dialog box. Use this button to add a new multicast group entry at the bottom of the table.
- **Edit**—Opens the [Multicast Group](#) dialog box. Use this button to change the information for the selected multicast group entry.
- **Delete**—Removes the selected multicast group entry from the table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |



## CHAPTER 13

# DHCP, DNS and WCCP Services

---

A DHCP server provides network configuration parameters, such as IP addresses, to DHCP clients. The security appliance can provide DHCP server or DHCP relay services to DHCP clients attached to security appliance interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface.

The Domain Name System (DNS) is the system in the Internet that maps names of objects (usually hostnames) into IP numbers or other resource record values. The namespace of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain. DNS client services allows you to specify DNS servers to which the security appliance sends DNS requests, request timeout period, and other parameters.

Dynamic DNS (DDNS) update integrates DNS with DHCP. The two protocols are complementary: DHCP centralizes and automates IP address allocation; DDNS update automatically records the association between assigned addresses and hostnames at pre-defined intervals. DDNS allows frequently changing address-hostname associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention.

For information about configuring these services, see the following sections:

- [DHCP Relay](#)
- [DHCP Server](#)
- [DNS Client](#)
- [Dynamic DNS](#)
- [WCCP](#)

## DHCP Relay

The DHCP Relay pane lets you configure DHCP relay services on the security appliance. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface. To configure DHCP relay, you need to specify at least one DHCP relay global server and then enable a DHCP relay agent on the interface receiving DHCP requests.

### Restrictions

- You cannot enable a DHCP relay agent on an interface that has a DHCP relay global server configured for it.
- The DHCP relay agent works only with external DHCP servers; it will not forward DHCP requests to a security appliance interface configured as a DHCP server.

### Prerequisites

Before you can enable a DHCP relay agent on an interface, you must have at least one DHCP relay global server in the configuration or DHCP relay interface server.

### Fields

- DHCP Relay Agent—*Display only*. Contains the fields for configuring the DHCP relay agent.
  - Interface—Displays the interface ID. Double-clicking the interface opens the Edit DHCP Relay Agent Settings dialog box, where you can enable the DHCP relay agent and configure the relay agent parameters.



**Note** You can double-click anywhere in the row for a particular interface to open the dialog box for that interface.

- DHCP Relay Enabled—Indicates whether the DHCP relay agent is enabled on the interface. This column displays “Yes” if the DHCP relay agent is enabled or “No” if the DHCP relay agent is not enabled on the interface.
- Set Route—Indicates whether the DHCP relay agent is configured to modify the default router address in the information returned from the DHCP server. This column display “Yes” if the DHCP relay agent is configured to change the default router address to the interface address or “No” if the DHCP relay agent does not modify the default router address.
- Edit—Opens the Edit DHCP Relay Agent Settings dialog box, where you can enable the DHCP relay agent and configure the relay agent parameters.
- DHCP Relay Global Server—Contains the fields for configuring the DHCP relay global servers.
  - Server—*Display only*. Displays the IP address of a configured, external DHCP server. Double-clicking a server address opens the DHCP Relay - Edit DHCP Server dialog box, where you can edit the DHCP relay global server settings.
  - Interface—*Display only*. Display the interface the specified DHCP server is attached to.
  - Add—Opens the DHCP Relay - Add DHCP Server dialog box, where you can specify a new DHCP relay global server. You can define up to 4 DHCP relay global servers on the security appliance. This button is unavailable if you already have 4 DHCP relay global servers defined.
  - Edit—Opens the DHCP Relay - Edit DHCP Server dialog box, where you can edit the DHCP relay global server settings.
  - Delete—Removes the selected DHCP relay global server. The server is removed from the security appliance configuration when you apply or save your changes.
  - Timeout—Specifies the amount of time, in seconds, allowed for DHCP address negotiation. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit DHCP Relay Agent Settings

You can enable the DHCP relay agent and configure the relay agent parameters for the selected interface in the Edit DHCP Relay Agent Settings dialog box.

### Restrictions

- You cannot enable a DHCP relay agent on an interface that has a DHCP relay global server configured for it.
- You cannot enable a DHCP relay agent on a security appliance that has DHCP server configured on an interface.

### Prerequisites

Before you can enable a DHCP relay agent on an selected interface, you must have at least one DHCP relay global server in the configuration.

### Fields

- Enable DHCP Relay Agent—When checked, enables the DHCP relay agent on the selected interface. You must have a DHCP relay global server defined before enabling the DHCP relay agent.
- Set Route—Specifies whether the DHCP relay agent is configured to modify the default router address in the information returned from the DHCP server. When this check box is checked, the DHCP relay agent substitutes the address of the selected interface for the default router address in the information returned from the DHCP server.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Global DHCP Relay Server

Define new global DHCP relay servers in the DHCP Relay - Add DHCP Server dialog box or edit existing server information in the DHCP Relay - Edit DHCP Server dialog box. You can define up to 4 DHCP relay global servers.

### Restrictions

You cannot define a global DHCP relay server on an interface with a DHCP server enabled on it.

### Fields

- DHCP Server—Specifies the IP address of the external DHCP server to which DHCP requests are forwarded.
- Interface—Specifies the interface through which DHCP requests are forwarded to the external DHCP server.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## DHCP Server

The DHCP Server pane lets you configure the security appliance interfaces as DHCP servers. You can configure one DHCP server per interface on the security appliance.



### Note

You cannot configure a DHCP server on an interface that has DHCP relay configured on it. For more information about DHCP relay, see [DHCP Relay](#).

### Fields

- Interface—*Display only*. Displays the interface ID. Double-clicking the interface ID opens the Edit DHCP Server dialog box, where you can enable DHCP on and assign a DHCP address pool to the selected interface.



### Note

You can double-click anywhere in the row for a particular interface to open the dialog box for that interface.

- DHCP Enabled—*Display only*. Indicates whether DHCP is enabled on the interface. This column displays “Yes” if DHCP is enabled or “No” if DHCP is not enabled on the interface.
- Address Pool—*Display only*. Displays the range of IP addresses assigned to the DHCP address pool.
- DNS Servers—*Display only*. Displays the DNS servers configured for the interface.
- WINS Servers—*Display only*. Displays the WINS servers configured for the interface.
- Domain Name—*Display only*. Displays the domain name of the interface.
- Ping Timeout—*Display only*. Displays time in milliseconds that the security appliance will wait for an ICMP ping response on the interface.
- Lease Length—*Display only*. Displays the duration of time that the DHCP server configured on the interface allows DHCP clients to use the an assigned IP address.
- Auto Interface—*Display only*. Displays the interface on a DHCP client providing DNS, WINS, and domain name information for automatic configuration.
- Options—*Display only*. Displays advanced DHCP options configured for the interface.
- Dynamic DNS Settings—*Display only*. Displays
- Edit—Opens the Edit DHCP Server dialog box for the selected interface. You can enable DHCP and specify the DHCP address pool in the Edit DHCP Server dialog box.
- Global DHCP Options—Contains optional DHCP parameters.



- Enable Auto-configuration from interface—Check this check box to enable DHCP auto configuration and select the interface from the menu.

DHCP auto configuration causes the DHCP server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client running on the specified interface. If any of the information obtained through auto configuration is also specified manually in the Other DHCP Options area, the manually specified information takes precedence over the discovered information.

- DNS Server 1—(Optional) Specifies the IP address of the primary DNS server for a DHCP client.
- DNS Server 2—(Optional) Specifies the IP address of the alternate DNS server for a DHCP client.
- Domain Name—(Optional) Specifies the DNS domain name for DHCP clients. Enter a valid DNS domain name, for example example.com.
- Lease Length—(Optional) Specifies the amount of time, in seconds, that the client can use its allocated IP address before the lease expires. Valid values range from 300 to 1048575 seconds. The default value is 3600 seconds (1 hour).
- Primary WINS Server—(Optional) Specifies the IP address of the primary WINS server for a DHCP client.
- Secondary WINS Server—(Optional) Specifies the IP address of the alternate WINS server for a DHCP client.
- Ping Timeout—(Optional) To avoid address conflicts, the security appliance sends two ICMP ping packets to an address before assigning that address to a DHCP client. The Ping Timeout field specifies the amount of time, in milliseconds, that the security appliance waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.
- Advanced—Opens the [Advanced DHCP Options](#) dialog box, where you can specify DHCP options and their parameters.
- Dynamic DNS Settings for DHCP Server—In this area, you can configure the DDNS update settings for the DHCP server.
  - Update DNS Clients—Check this check box to specify that, besides the default action of updating the client PTR resource records, the DHCP server should also perform the following update actions (if selected):
  - Update Both Records—Check this check box to specify that the DHCP server should update both the A and PTR RRs.
  - Override Client Settings—Check this check box to specify that the DHCP server actions should override any update actions requested by the DHCP client.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit DHCP Server

You can enable DHCP and specify the DHCP address pool for the selected interface in the Edit DHCP Server dialog box.

### Fields

- **Enable DHCP Server**—Check this check box to enable the DHCP server on the selected interface. Uncheck this check box to disable DHCP on the selected interface. Disabling the DHCP server on the selected interface does not clear the specified DHCP address pool.
- **DHCP Address Pool**—Enter the IP address pool used by the DHCP server. Enter the range of IP addresses from lowest to highest. The range of IP addresses must be on the same subnet as the selected interface and cannot contain the IP address of the interface itself.
- **Optional Parameters**—You can optionally configure the following parameters for the DHCP server:
  - **DNS Server 1**—Enter the IP address of the primary DNS server for a DHCP client.
  - **DNS Server 2**—Enter the IP address of the alternate DNS server for a DHCP client.
  - **Domain Name**—Enter the DNS domain name for DHCP clients. Enter a valid DNS domain name, for example example.com.
  - **Lease Length**—Enter the amount of time, in seconds, that the client can use its allocated IP address before the lease expires. Valid values range from 300 to 1048575 seconds. The default value is 3600 seconds (1 hour).
  - **Primary WINS Server**—Enter the IP address of the primary WINS server for a DHCP client.
  - **Secondary WINS Server**—Enter the IP address of the alternate WINS server for a DHCP client.
  - **Ping Timeout**—Enter the amount of time, in milliseconds, that the security appliance waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.
  - **Enable Auto-configuration on interface**—Check this check box to enable DHCP auto-configuration and select the interface from the menu.
  - **Advanced**—Opens the [Advanced DHCP Options](#) dialog box, where you can specify DHCP options and their parameters.
- **Dynamic DNS Settings for DHCP Server**—In this area, you can configure the DDNS update settings for the DHCP server.
  - **Update DNS Clients**—Check this check box to specify that, besides the default action of updating the client PTR resource records, the DHCP server should also perform the following update actions (if selected):
  - **Update Both Records**—Check this check box to specify that the DHCP server should update both the A and PTR RRs.
  - **Override Client Settings**—Check this check box to specify that DHCP server actions should override any update actions requested by the DHCP client.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Advanced DHCP Options

The Advanced DHCP Options dialog box lets you configure DHCP option parameters. You use DHCP options to provide additional information to DHCP clients. For example, DHCP option 150 and DHCP option 66 provide TFTP server information to Cisco IP Phones and Cisco IOS routers.

You can use that advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients. You can also use the DHCP auto configuration setting to obtain these values or manually specify them on the [DHCP Server](#) pane. When you use more than one method to specify this information, the information is passed to DHCP clients with the following preference:

1. Manually configured settings.
2. Advanced DHCP Options settings.
3. DHCP auto configuration.

For example, you can manually define the domain name that you want the DHCP clients to receive, and then enable DHCP auto configuration. Although DHCP auto configuration will discover the domain along with the DNS and WINS servers, the manually-defined domain name is passed to DHCP clients with the discovered DNS and WINS server names. The domain name discovered by the DHCP auto configuration process is discarded in favor of the manually-defined domain name.

### Fields

- Option to be Added—Contains the fields used to configure a DHCP option.
  - Choose the option code—Lists the available option codes. All DHCP options (options 1 through 255) are supported except 1, 12, 50–54, 58–59, 61, 67, and 82. Choose the option that you want to configure.

Some options are standard. For standard options, the option name is shown in parentheses after the option number and the option parameters are limited to those supported by the option. For all other options, only the option number is shown and you must choose the appropriate parameters to supply with the option.

For standard DHCP options, only the supported option value type is available. For example, if you choose DHCP Option 2 (Time Offset), you can only supply a hexadecimal value for the option. For all other DHCP options, all of the option value types are available and you must choose the appropriate options value type.
- Option Data—These options specify the type of information the option returns to the DHCP client. For standard DHCP options, only the supported option value type is available. For all other DHCP options, all of the option value types are available.
- IP Address—Choosing this value specifies that an IP address is returned to the DHCP client. You can specify up to two IP addresses.

**Note**

The name of the associated IP Address fields can change based on the DHCP option you chose. For example, if you choose DHCP Option 3 (Router), the fields change name to Router 1 and Router 2.

- IP Address 1—An IP address in dotted-decimal notation.
- IP Address 2—(Optional) An IP address in dotted-decimal notation.
- ASCII—Choose this option specifies that an ASCII value is returned to the DHCP client.

**Note**

The name of the associated Data field can change based on the DHCP option you chose. For example, if you choose DHCP Option 14 (Merit Dump File), the associated Data field changes name to File Name.

- Data—An ASCII character string. The string cannot include white space.
- Hex—Selecting this option specifies that a hexadecimal value is returned to the DHCP client.

**Note**

The name of the associated Data field can change based on the DHCP option you chose. For example, if you choose DHCP Option 2 (Time Offset), the associated Data field becomes the Offset field.

- Data—A hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
- Add—Adds the configured option to the DHCP option table.
- Delete—Removes the selected option from the DHCP option table.
- DHCP option table—Lists the DHCP options that have been configured.
  - Option Code—Shows the DHCP option code. For standard DHCP options, the option name appears in parentheses next to the option code.
  - Option Data—Shows the parameters that have been configured for the selected option.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# DNS Client

The DNS Client pane shows the DNS server groups and DNS lookup information for the security appliance, so it can resolve server names to IP addresses in your Clientless SSL VPN configuration or certificate configuration. Other features that define server names (such as AAA) do not support DNS resolution. In those cases, you must enter the IP address or manually resolve the name to an IP address by adding the server name in the [Network Object Groups](#) pane.

## Fields

- **DNS Server Groups**—Displays and manages the DNS server list. There can be up to six addresses to which DNS requests can be forwarded. The security appliance tries each DNS server in order until it receives a response. You must enable DNS on at least one interface in the DNS Lookup area before you can add a DNS server. The contents of the table in this area are as follows:
  - **Name**—*Display only*. Shows the name of each configured DNS server group.
  - **Servers**—*Display only*. Shows the IP addresses of the configured servers.
  - **Timeout**—*Display only*. Shows the number of seconds to wait before trying the next DNS server in the list, between 1 and 30 seconds. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles.
  - **Retries**—*Display only*. Shows the number of seconds to wait before trying the next DNS server in the list.
  - **Domain Name**—*Display only*. Shows the number of times the security appliance retries the request.
- **DNS Lookup**—Enables or disables DNS lookup on an interface.
  - **Interface**—*Display only*. Lists all interface names.
  - **DNS Enabled**—*Display only*. Shows whether an interface supports DNS lookup, Yes or No.
  - **Disable**—Disables DNS lookup for the selected interface.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# Add/Edit DNS Server Group

The Add or Edit DNS Server Group pane lets you specify or modify one or more DNS servers for the security appliance so it can resolve server names to IP addresses in your Clientless SSL VPN configuration or certificate configuration. Other features that define server names (such as AAA) do not support DNS resolution. For those, you must enter the IP address or manually resolve the name to an IP address by adding the server name in the [Network Object Groups](#) pane.

**Fields**

- **Name**—Specifies the server name. For the Edit function, this field is *Display only*.
- **DNS Servers**—Manages the DNS server list. You can specify up to six addresses to which DNS requests can be forwarded. The security appliance tries each DNS server in order until it receives a response. You must enable DNS on at least one interface in the DNS Lookup area before you can add a DNS server.
  - **Server to be Added**—Specifies the DNS server IP address.
  - **Add**—Adds a DNS server to the bottom of the list.
  - **Delete**—Deletes the selected DNS server from the list.
  - **Servers**—*Display only*. Shows the DNS server list.
  - **Move Up**—Moves the selected DNS server up the list.
  - **Move down**—Moves the selected DNS server down the list.
- **Timeout**—Specifies the number of seconds to wait before trying the next DNS server in the list, between 1 and 30 seconds. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles.
- **Retries**—Sets the number of times the security appliance retries the request. The range is 1 through 10 retries.
- **Domain Name**—(Optional) Specifies the DNS domain name for the server. Enter a valid DNS domain name; for example example.com.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Dynamic DNS

Dynamic DNS provides address and domain name mappings so hosts can find each other even though their DHCP-assigned IP addresses change frequently. The DDNS name and address mappings are held on the DHCP server in two resource records: the A RR contains the name to IP address mapping while the PTR RR maps addresses to names. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.

The Dynamic DNS pane shows the configured DDNS update methods and the interfaces configured for DDNS. By automatically records the association between assigned addresses and hostnames at pre-defined intervals, DDNS allows frequently changing address-hostname associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention.

### Fields

- Update Methods—Lists the DDNS update methods that are configured on the security appliance. This table includes:
  - Method Name—*Display only*. Shows the user-defined name for the DDNS update method.
  - Interval—*Display only*. Shows the time between DNS update attempts configured for the update method.
  - Update DNS Server Records—*Display only*. Shows whether the method updates both the A resource record (name to IP address) and the PTR resource record (IP address to name), or neither record.
  - Add/Edit—Displays the Add/Edit Dynamic DNS Update Methods dialog box.
  - Delete—Removes the currently selected update method from the table.
- Dynamic DNS Interface Settings—Lists the DDNS settings for each interface configured for DDNS.
  - Interface—*Display only*. Shows the names of the security appliance interfaces configured for DDNS.
  - Method Name—*Display only*. Shows the update methods assigned to each interface.
  - Hostname—*Display only*. Shows the hostname of the DDNS client.
  - Update DHCP Server Records—*Display only*. Shows whether the interface updates both the A and PTR resource records or neither.
  - Add/Edit—Displays the Add/Edit Dynamic DNS Interface Settings dialog box.
  - Delete—Removes the DDNS update settings for the selected interface.
- DHCP Clients Update DNS Records—This is the global setting specifying which records the DHCP client requests to be updated by the DHCP server. Click one of the following radio buttons:
  - Default (PTR Records) to specify that the client request PTR record updating by the server  
–or–
  - Both (PTR Records and A Records) to specify that the client request both the A and PTR DNS resource records by the server  
–or–
  - None to specify that the client request no updates by the server

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | •        | —      |

## Add/Edit Dynamic DNS Update Methods

The Add/Edit Dynamic DNS Update Methods dialog box lets you add a new method or edit a previously added method. You can specify the method name (if adding a method), specify the interval between DDNS update attempts, and specify whether the DDNS client attempts to update both or neither of the two DNS records, the A record and the PTR record.

### Fields

- **Name**—If you are adding a method, enter then name of the new method in this field. If you are editing an existing method, this field is *display-only* and shows the name of the method selected for editing.
- **Update Interval**—Specifies the time to elapse between update attempts. The interval ranges from 0 to nearly one year.
  - **Days**—Choose the number of days between update attempts from 0 to 364.
  - **Hours**—Choose the number of hours (in whole numbers) between update attempts from 0 to 23.
  - **Minutes**—Choose the number of minutes (in whole numbers) between update attempts from 0 to 59.
  - **Seconds**—Choose the number of minutes (in whole numbers) between update attempts from 0 to 59.
  - **Update Records**—Click Both (A and PTR Records) for the client to attempt updates to both the A and PTR DNS resource records, or click A Records Only to update just the A records. This is the individual method setting for DNS server records updated by the client.

These units are additive. That is, if you enter 0 days, 0 hours, 5 minutes and 15 seconds, the update method will attempt an update every 5 minutes and 15 seconds for as long as the method is active.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | •        | —      |

## Add/Edit Dynamic DNS Interface Settings

The Add/Edit Dynamic DNS Interface Settings allows you to configure DDNS on a security appliance interface. You can assign an update method, specify the hostname, and configure DHCP server updating of both the A and PTR records by the client or neither.

### Fields

- **Interface**—Choose an interface on which to configure DDNS from the menu.
- **Update Method**—Choose an available DDNS update method from the menu.
- **Hostname**—Enter the hostname of the DDNS client.



- DHCP Client—This area allows you to specify that the DHCP client updates both the A and PTR DNS records or neither. This interface setting overrides the global setting at Configuration > Properties > DNS > Dynamic DNS
- DHCP Client Updates DNS Records—Click one of the following radio buttons:
  - Default (PTR Records only) to specify that the client request only PTR record updating by the server
  - or–
  - Both (PTR Records and A Records) to specify that the client request both the A and PTR DNS resource records by the server
  - or–
  - None to specify that the client request no updates by the server



**Note** DHCP must be enabled on the selected interface for this action to be effective.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | •        | —      |

## WCCP

The Web Cache Communication Protocol (WCCP) feature lets you specify WCCP service groups and redirect web cache traffic. The feature transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.

## WCCP Service Groups

The Service Groups pane lets you allocate space and enable support of the specified Web Cache Communication Protocol (WCCP) service group.

### Fields

- Service—Displays the service group name or service group number for WCCP support.
- Redirect List—Displays the name of the access list that controls traffic redirected to a specific service group.
- Group List—Displays the name of the access list that determines which web caches are allowed to participate in the service group.

## Add or Edit WCCP Service Group

The Add or Edit Service Group dialog box lets you change the service group parameters for a configured service group.

### Fields

- **Service**—Specifies the service group. You can specify the web cache service, or the identification number of the service.
- **Web Cache**—Specifies the web cache service. The maximum number of services, including those specified with a dynamic service identifier is 256.
- **Dynamic Service Number**—Enter the dynamic service identifier, which means the service definition is dictated by the cache. Valid dynamic service numbers are 0 to 254, and are used as the name of the service group.
- **Redirect List**—Lets you choose the predefined access list that controls traffic redirected to this service group.
- **Group List**—Lets you choose the predefined access list that determines which web caches are allowed to participate in the service group. Only extended ACLs are allowed.
- **Password**—Enter a password up to seven characters long, which is used for MD5 authentication for messages received from the service group.
- **Confirm Password**—Reenter the password.
- **Manage**—Click to open the ACL Manager window, where you can create or change the ACL.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

## Redirection

The Redirection pane lets you enable packet redirection on the ingress of an interface using WCCP.

### Fields

- **Interface**—Displays the interface on which WCCP redirection is enabled.
- **Service Group**—Displays the name of the service group configured for WCCP.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

## Add or Edit WCCP Redirection

The Redirection pane lets you add or change packet redirection on the ingress of an interface using WCCP.

### Fields

- Interface—Choose the interface on which to enable WCCP redirection.
- Service Group—Choose the service group.
- New—Opens the Add Service Group dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |





# CHAPTER 14

## Configuring AAA Servers and the Local Database

---

This chapter describes support for AAA (pronounced “triple A”) and how to configure AAA servers and the local database.

This chapter includes the following sections:

- [AAA Overview, page 14-1](#)
- [AAA Server and Local Database Support, page 14-3](#)
- [Configuring AAA Server Groups, page 14-9](#)
- [Testing Server Authentication and Authorization, page 14-16](#)
- [Adding a User Account, page 14-17](#)
- [Configuring LDAP Attribute Maps, page 14-21](#)
- [Adding an Authentication Prompt, page 14-22](#)

### AAA Overview

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting).

AAA provides an extra level of protection and control for user access than using access lists alone. For example, you can create an access list allowing all outside users to access Telnet on a server on the DMZ network. If you want only some users to access the server and you might not always know IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the security appliance. (The Telnet server enforces authentication, too; the security appliance prevents unauthorized users from attempting to access the server.)

You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

This section includes the following topics:

- [About Authentication, page 14-2](#)
- [About Authorization, page 14-2](#)
- [About Accounting, page 14-2](#)

## About Authentication

Authentication controls access by requiring valid user credentials, which are typically a username and password. You can configure the security appliance to authenticate the following items:

- All administrative connections to the security appliance including the following sessions:
  - Telnet
  - SSH
  - Serial console
  - ASDM (using HTTPS)
  - VPN management access
- The **enable** command
- Network access
- VPN access

## About Authorization

Authorization controls access *per user* after users authenticate. You can configure the security appliance to authorize the following items:

- Management commands
- Network access
- VPN access

Authorization controls the services and commands available to each authenticated user. Were you not to enable authorization, authentication alone would provide the same access to services for all authenticated users.

If you need the control that authorization provides, you can configure a broad authentication rule, and then have a detailed authorization configuration. For example, you authenticate inside users who attempt to access any server on the outside network and then limit the outside servers that a particular user can access using authorization.

The security appliance caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the security appliance does not resend the request to the authorization server.

## About Accounting

Accounting tracks traffic that passes through the security appliance, enabling you to have a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic per IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

# AAA Server and Local Database Support

The security appliance supports a variety of AAA server types and a local database that is stored on the security appliance. This section describes support for each AAA server type and the local database.

This section contains the following topics:

- [Summary of Support, page 14-3](#)
- [RADIUS Server Support, page 14-4](#)
- [TACACS+ Server Support, page 14-4](#)
- [SDI Server Support, page 14-5](#)
- [NT Server Support, page 14-5](#)
- [Kerberos Server Support, page 14-5](#)
- [LDAP Server Support, page 14-6](#)
- [SSO Support for WebVPN with HTTP Forms, page 14-7](#)
- [Local Database Support, page 14-8](#)

## Summary of Support

[Table 14-1](#) summarizes the support for each AAA service by each AAA server type, including the local database. For more information about support for a specific AAA server type, refer to the topics following the table.

**Table 14-1 Summary of AAA Support**

| AAA Service                 | Database Type    |                  |         |                  |     |          |      |                  |
|-----------------------------|------------------|------------------|---------|------------------|-----|----------|------|------------------|
|                             | Local            | RADIUS           | TACACS+ | SDI              | NT  | Kerberos | LDAP | HTTP Form        |
| <b>Authentication of...</b> |                  |                  |         |                  |     |          |      |                  |
| VPN users                   | Yes              | Yes              | Yes     | Yes              | Yes | Yes      | Yes  | Yes <sup>1</sup> |
| Firewall sessions           | Yes              | Yes              | Yes     | Yes              | Yes | Yes      | Yes  | No               |
| Administrators              | Yes              | Yes              | Yes     | Yes <sup>2</sup> | Yes | Yes      | Yes  | No               |
| <b>Authorization of...</b>  |                  |                  |         |                  |     |          |      |                  |
| VPN users                   | Yes              | Yes              | No      | No               | No  | No       | Yes  | No               |
| Firewall sessions           | No               | Yes <sup>3</sup> | Yes     | No               | No  | No       | No   | No               |
| Administrators              | Yes <sup>4</sup> | No               | Yes     | No               | No  | No       | No   | No               |
| <b>Accounting of...</b>     |                  |                  |         |                  |     |          |      |                  |
| VPN connections             | No               | Yes              | Yes     | No               | No  | No       | No   | No               |
| Firewall sessions           | No               | Yes              | Yes     | No               | No  | No       | No   | No               |
| Administrators              | No               | Yes <sup>5</sup> | Yes     | No               | No  | No       | No   | No               |

1. HTTP Form protocol supports single sign-on authentication for WebVPN users only.

2. SDI is not supported for HTTP administrative access.

3. For firewall sessions, RADIUS authorization is supported with user-specific access lists only, which are received or specified in a RADIUS authentication response.

4. Local command authorization is supported by privilege level only.
5. Command accounting is available for TACACS+ only.

## RADIUS Server Support

The security appliance supports RADIUS servers.

This section contains the following topics:

- [Authentication Methods, page 14-4](#)
- [Attribute Support, page 14-4](#)
- [RADIUS Authorization Functions, page 14-4](#)

### Authentication Methods

The security appliance supports the following authentication methods with RADIUS:

- PAP—For all connection types.
- CHAP—For L2TP-over-IPSec.
- MS-CHAPv1—For L2TP-over-IPSec.
- MS-CHAPv2—For L2TP-over-IPSec, and for regular IPSec remote access connections when the password management feature is enabled.

### Attribute Support

The security appliance supports the following sets of RADIUS attributes:

- Authentication attributes defined in RFC 2138.
- Accounting attributes defined in RFC 2139.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868.
- Cisco IOS VSAs, identified by RADIUS vendor ID 9.
- Cisco VPN-related VSAs, identified by RADIUS vendor ID 3076.
- Microsoft VSAs, defined in RFC 2548.

### RADIUS Authorization Functions

The security appliance can use RADIUS servers for user authorization for network access using dynamic access lists or access list names per user. To implement dynamic access lists, you must configure the RADIUS server to support it. When the user authenticates, the RADIUS server sends a downloadable access list or access list name to the security appliance. Access to a given service is either permitted or denied by the access list. The security appliance deletes the access list when the authentication session expires.

## TACACS+ Server Support

The security appliance supports TACACS+ authentication with ASCII, PAP, CHAP, and MS-CHAPv1.



## SDI Server Support

The RSA SecurID servers are also known as SDI servers.

This section contains the following topics:

- [SDI Version Support, page 14-5](#)
- [Two-step Authentication Process, page 14-5](#)
- [SDI Primary and Replica Servers, page 14-5](#)

### SDI Version Support

The security appliance supports SDI Version 5.0 and 6.0. SDI uses the concepts of an SDI primary and SDI replica servers. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended.

A version 5.0 or 6.0 SDI server that you configure on the security appliance can be either the primary or any one of the replicas. See the “[SDI Primary and Replica Servers](#)” section on page 14-5 for information about how the SDI agent selects servers to authenticate users.

### Two-step Authentication Process

SDI version 5.0 and 6.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two security appliances using the same authentication servers simultaneously. After a successful username lock, the security appliance sends the passcode.

### SDI Primary and Replica Servers

The security appliance obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The security appliance then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

## NT Server Support

The security appliance supports Microsoft Windows server operating systems that support NTLM version 1, collectively referred to as NT servers.

**Note**

NT servers have a maximum length of 14 characters for user passwords. Longer passwords are truncated. This is a limitation of NTLM version 1.

## Kerberos Server Support

The security appliance supports 3DES, DES, and RC4 encryption types.

**Note**

The security appliance does not support changing user passwords during tunnel negotiation. To avoid this situation happening inadvertently, disable password expiration on the Kerberos/Active Directory server for users connecting to the security appliance.

## LDAP Server Support

This section describes LDAP server support, and includes the following topics:

- [Authentication with LDAP, page 14-6](#)
- [Securing LDAP Authentication with SASL, page 14-6](#)
- [LDAP Server Types, page 14-7](#)
- [Authorization with LDAP for VPN, page 14-7](#)

### Authentication with LDAP

During authentication, the security appliance acts as a client proxy to the LDAP server for the user, and authenticates to the LDAP server in either plain text or using the Simple Authentication and Security Layer (SASL) protocol. By default, the security appliance passes authentication parameters, usually a username and password, to the LDAP server in plain text. Whether using SASL or plain text, you can secure the communications between the security appliance and the LDAP server with SSL.

**Note**

If you do not configure SASL, we strongly recommend that you secure LDAP communications with SSL.

When user LDAP authentication has succeeded, the LDAP server returns the attributes for the authenticated user. For VPN authentication, these attributes generally include authorization data which is applied to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

### Securing LDAP Authentication with SASL

The security appliance supports the following SASL mechanisms, listed in order of increasing strength:

- Digest-MD5 — The security appliance responds to the LDAP server with an MD5 value computed from the username and password.
- Kerberos — The security appliance responds to the LDAP server by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.

You can configure the security appliance and LDAP server to support any combination of these SASL mechanisms. If you configure multiple mechanisms, the security appliance retrieves the list of SASL mechanisms configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the security appliance and the server. For example, if both the LDAP server and the security appliance support both mechanisms, the security appliance selects Kerberos, the stronger of the mechanisms.

## LDAP Server Types

The security appliance supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server), the Microsoft Active Directory, and other LDAPv3 directory servers.

By default, the security appliance auto-detects whether it is connected to a Microsoft Active Directory, a Sun LDAP directory server, or a generic LDAPv3 directory server. However, if auto-detection fails to determine the LDAP server type, and you know the server is either a Microsoft, Sun or generic LDAP server, you can manually configure the server type.



### Note

- Sun—The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—The security appliance does not support password management with a generic LDAPv3 directory server.

## Authorization with LDAP for VPN

When user LDAP authentication for VPN access has succeeded, the security appliance queries the LDAP server which returns LDAP attributes. These attributes generally include authorization data that applies to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

There may be cases, however, where you require authorization from an LDAP directory server that is separate and distinct from the authentication mechanism. For example, if you use an SDI or certificate server for authentication, no authorization information is passed back. For user authorizations in this case, you can query an LDAP directory after successful authentication, accomplishing authentication and authorization in two steps.

## SSO Support for WebVPN with HTTP Forms

The security appliance can use the HTTP Form protocol for single sign-on (SSO) authentication of WebVPN users only. Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and Web servers. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

In addition to the HTTP Form protocol, WebVPN administrators can choose to configure SSO with the HTTP Basic and NTLM authentication protocols (the **auto-signon** command), or with Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder) as well. For an in-depth discussion of configuring SSO with either HTTP Forms, **auto-signon** or SiteMinder, see the [Clientless SSL VPN](#) chapter.

## Local Database Support

The security appliance maintains a local database that you can populate with user profiles.

This section contains the following topics:

- [User Profiles, page 14-8](#)
- [Fallback Support, page 14-8](#)

### User Profiles

User profiles contain, at a minimum, a username. Typically, a password is assigned to each username, although passwords are optional.

The **username attributes** command lets you enter the username mode. In this mode, you can add other information to a specific user profile. The information you can add includes VPN-related attributes, such as a VPN session timeout value.

### Fallback Support

The local database can act as a fallback method for several functions. This behavior is designed to help you prevent accidental lockout from the security appliance.

For users who need fallback support, we recommend that their usernames and passwords in the local database match their usernames and passwords in the AAA servers. This provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the service, using usernames and passwords on AAA servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

The local database supports the following fallback functions:

- **Console and enable password authentication**—When you use the **aaa authentication console** command, you can add the **LOCAL** keyword after the AAA server group tag. If the servers in the group all are unavailable, the security appliance uses the local database to authenticate administrative access. This can include enable password authentication, too.
- **Command authorization**—When you use the **aaa authorization command** command, you can add the **LOCAL** keyword after the AAA server group tag. If the TACACS+ servers in the group all are unavailable, the local database is used to authorize commands based on privilege levels.
- **VPN authentication and authorization**—VPN authentication and authorization are supported to enable remote access to the security appliance if AAA servers that normally support these VPN services are unavailable. The **authentication-server-group** command, available in tunnel-group general attributes mode, lets you specify the **LOCAL** keyword when you are configuring attributes of a tunnel group. When VPN client of an administrator specifies a tunnel group configured to fallback to the local database, the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured with the necessary attributes.

# Configuring AAA Server Groups

If you want to use an external AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group per AAA protocol and add one or more servers to each group. You identify AAA server groups by name. Each server group is specific to one type of server: Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

The security appliance contacts the first server in the group. If that server is unavailable, the security appliance contacts the next server in the group, if configured. If all servers in the group are unavailable, the security appliance tries the local database if you configured it as a fallback method (management authentication and authorization only). If you do not have a fallback method, the security appliance continues to try the AAA servers.

This section includes the following procedures:

- [Adding a Server Group, page 14-9](#)
- [Adding a Server to a Group, page 14-10](#)
- [AAA Server Parameters, page 14-11](#)

## Adding a Server Group

To add a server group, perform the following steps:

**Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click **Add**.

The Add AAA Server Group dialog box appears.

**Step 2** In the Server Group field, add a name for the group.

**Step 3** From the Protocol drop-down list, choose the server type:

- **RADIUS**
- **TACACS+**
- **SDI**
- **NT Domain**
- **Kerberos**
- **LDAP**
- **HTTP Form**

**Step 4** In the Accounting Mode field click the radio button for the mode you want to use (**Simultaneous** or **Single**).

In Single mode, the security appliance sends accounting data to only one server.

In Simultaneous mode, the security appliance sends accounting data to all servers in the group.



**Note** This option is not available for the HTTP Form protocol.

**Step 5** In the Reactivation Mode field, click the radio button for the mode you want to use (**Depletion** or **Timed**).

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.

In Timed mode, failed servers are reactivated after 30 seconds of down time.



**Note** This option is not available for the HTTP Form protocol.

**Step 6** If you chose Depletion reactivation mode, add a time interval in the Dead Time field.  
The Dead Time is the duration of time, in minutes, to elapse between the disabling of the last server in a group and the subsequent reenabling of all servers.

**Step 7** In the Max Failed Attempts field, add the number of failed attempts permitted.  
This option sets the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive.



**Note** This option is not available for the HTTP Form protocol.

**Step 8** Click **OK**.  
The dialog box closes and the server group is added to the AAA server groups table.

**Step 9** In the AAA Server Groups dialog box, click **Apply** to save the changes.  
The changes are saved.

## Adding a Server to a Group

To add a AAA server to a group, perform the following steps:

- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click the server group to which you want to add a server.  
The row is highlighted in the table.
- Step 2** In the Servers in the Selected Group area (lower pane), click **Add**.  
The Add AAA Server Group dialog box appears for the server group.
- Step 3** From the Interface Name drop-down menu, choose the interface name where the authentication server resides.
- Step 4** In the Server Name or IP Address field, add either a server name or IP address for the server you are adding to the group.
- Step 5** In the Timeout field, either add a timeout value or keep the default. The timeout is the duration of time, in seconds, that the security appliance waits for a response from the primary server before sending the request to the backup server.
- Step 6** The other parameters available depend on the server type. See the following sections for parameters unique to each server type:
  - [RADIUS Server Fields, page 14-11](#)
  - [TACACS+ Server Fields, page 14-13](#)
  - [SDI Server Fields, page 14-13](#)
  - [Windows NT Domain Server Fields, page 14-13](#)

- [Kerberos Server Fields, page 14-14](#)
- [LDAP Server Fields, page 14-14](#)
- [HTTP Form Server Fields, page 14-16](#)

**Step 7** Click **OK**.

The dialog box closes and the AAA server is added to the AAA server group.

**Step 8** In the AAA Server Groups pane, click **Apply** to save the changes.

The changes are saved.

---

## AAA Server Parameters


The following sections list the unique fields for each server type when adding a server to a server group (see the [“Adding a Server to a Group” section on page 14-10](#)):

- [RADIUS Server Fields, page 14-11](#)
- [TACACS+ Server Fields, page 14-13](#)
- [SDI Server Fields, page 14-13](#)
- [Windows NT Domain Server Fields, page 14-13](#)
- [Kerberos Server Fields, page 14-14](#)
- [LDAP Server Fields, page 14-14](#)
- [HTTP Form Server Fields, page 14-16](#)

## RADIUS Server Fields

The following table describes the unique fields for configuring RADIUS servers, for use with the [“Adding a Server to a Group” section on page 14-10](#).

| Field                      | Description                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Authentication Port | The server port to be used for authentication of users.<br>The default port is 1645.                                                                                                                                                                                                                     |
| Server Accounting Port     | The server port to be used for accounting of users.<br>The default port is 1646.                                                                                                                                                                                                                         |
| Retry Interval             | The duration of time, 1 to 10 seconds, that the security appliance waits between attempts to contact the server.                                                                                                                                                                                         |
| Server Secret Key          | The shared secret key used to authenticate the RADIUS server to the security appliance. The server secret you configure here should match the one configured on the RADIUS server. If you do not know the server secret, ask the RADIUS server administrator. The maximum field length is 64 characters. |

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Common Password     | <p>A case-sensitive password that is common among users who access this RADIUS <b>authorization</b> server through this security appliance. Be sure to provide this information to your RADIUS server administrator.</p> <p><b>Note</b> For an authentication RADIUS server (rather than authorization) do not configure a common password.</p> <p>If you leave this field blank, the users username is the password for accessing this RADIUS <b>authorization</b> server.</p> <p>Never use a RADIUS authorization server for authentication. Common passwords or usernames as passwords are less secure than assigning unique user passwords.</p> <p><b>Note</b> Although the password is required by the RADIUS protocol and the RADIUS server, users do not need to know it.</p>                                                                                                                                                                                                                                                                                                                                                                                 |
| ACL Netmask Convert | <p>How you want the security appliance to handle netmasks received in downloadable access lists.</p> <ul style="list-style-type: none"> <li>• Detect automatically: The security appliance attempts to determine the type of netmask expression used. If it detects a wildcard netmask expression, it converts it to a standard netmask expression;</li> </ul> <p></p> <p><b>Note</b> Because some wildcard expressions are difficult to detect clearly, this setting may misinterpret a wildcard netmask expression as a standard netmask expression.</p> <ul style="list-style-type: none"> <li>• Standard: The security appliance assumes downloadable access lists received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.</li> <li>• Wildcard: The security appliance assumes downloadable access lists received from the RADIUS server contain only wildcard netmask expressions and it converts them all to standard netmask expressions when the access lists are downloaded.</li> </ul> |



## TACACS+ Server Fields

The following table describes the unique fields for configuring TACACS+ servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

| Field             | Description                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Port       | The port to be used for this server.                                                                                                                                                                                                                                                                       |
| Server Secret Key | The shared secret key used to authenticate the TACACS+ server to the security appliance. The server secret you configure here should match the one configured on the TACACS+ server. If you do not know the server secret, ask the RADIUS server administrator. The maximum field length is 64 characters. |

## SDI Server Fields

The following table describes the unique fields for configuring SDI servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

| Field          | Description                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------|
| Server Port    | The TCP port number by which this server is accessed.                                                            |
| Retry Interval | The duration of time, 1 to 10 seconds, that the security appliance waits between attempts to contact the server. |

## Windows NT Domain Server Fields

The following table describes the unique fields for configuring Windows NT Domain servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

| Field             | Description                                                                                                                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Port       | Port number 139, or the TCP port number used by the security appliance to communicate with the Windows NT server.                                                                                                                                                                                                      |
| Domain Controller | The host name (no more than 15 characters) of the NT Primary Domain Controller for this server. For example, PDC01. You must enter a name, and it must be the correct host name for the server whose IP Address you added in the field, Authentication Server Address. If the name is incorrect, authentication fails. |

## Kerberos Server Fields

The following table describes the unique fields for configuring Kerberos servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Port    | Server port number 88, or the UDP port number over which the security appliance communicates with the Kerberos server.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Retry Interval | The duration of time, 1 to 10 seconds, that the security appliance waits between attempts to contact the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Realm          | <p>The name of the Kerberos realm, for example:</p> <ul style="list-style-type: none"> <li>example.com</li> <li>example.net</li> <li>example.org</li> </ul> <p>The maximum length is 64 characters. The following types of servers require that you enter the realm name in all uppercase letters:</p> <ul style="list-style-type: none"> <li>Windows 2000</li> <li>Windows XP</li> <li>Windows.NET</li> </ul> <p>You must enter this name, and it must be the correct realm name for the server whose IP address you entered in the Server IP Address field.</p> |

## LDAP Server Fields

The following table describes the unique fields for configuring LDAP servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

| Field                          | Description                                                                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable LDAP over SSL check box | <p>When checked, SSL secures communications between the security appliance and the LDAP server. Also called secure LDAP.</p> <p><b>Note</b> If you do not configure SASL protocol, we strongly recommend that you secure LDAP communications with SSL.</p> |
| Server Port                    | TCP port number 389, the port which the security appliance uses to access the LDAP server.                                                                                                                                                                 |
| Server type                    | <p>A drop-down list for choosing one of the following LDAP server types:</p> <ul style="list-style-type: none"> <li>Detect Automatically/Use Generic Type</li> <li>Microsoft</li> <li>Novell</li> <li>OpenLDAP</li> <li>Sun</li> </ul>                     |

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base DN                           | The Base Distinguished Name (DN), or location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example, OU=people, dc=cisco, dc=com.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Scope                             | The extent of the search the server should make in the LDAP hierarchy when it receives an authorization request. The available options are: <ul style="list-style-type: none"> <li>One Level: Searches only one level beneath the Base DN. This option is quicker.</li> <li>All Levels: Searches all levels beneath the Base DN; in other words, search the entire subtree hierarchy. This option takes more time.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Naming Attribute(s)               | The Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Login DN                          | The login Distinguished Name (DN), or the name of the directory object for security appliance authenticated binding. Examples are: <ul style="list-style-type: none"> <li>cn=Administrator</li> <li>cn=users</li> <li>ou=people</li> <li>dc=Example Corporation</li> <li>dc=com</li> </ul> For anonymous access, leave this field blank.<br>Some LDAP servers (including the Microsoft Active Directory server) require the security appliance to establish a handshake via authenticated binding before accepting requests for other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field defines the security appliance's authentication characteristics; these characteristics should correspond to those of a user with administration privileges. |
| Login Password                    | The login password. The characters you type are replaced with asterisks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| LDAP Attribute Map                | The LDAP attribute maps that you can apply to LDAP server. Used to map Cisco attribute names to user-defined attribute names and values. See the <a href="#">“Configuring LDAP Attribute Maps” section on page 14-21</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SASL MD5 authentication check box | When checked, the MD5 mechanism of the Simple Authentication and Security Layer (SASL) authenticates communications between the security appliance and the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SASL Kerberos authentication      | When checked, the Kerberos mechanism of the SASL secures authentication communications between the security appliance and the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Kerberos Server Group             | The Kerberos server or server group used for authentication. The Kerberos Server group option is disabled by default and is enabled only when SASL Kerberos authentication is chosen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## HTTP Form Server Fields

This area appears only when the selected server group uses HTTP Form, and only the server group name and the protocol are visible. Other fields are not available when using HTTP Form.

If you do not know what the following parameters are, use an HTTP header analyzer to extract the data from the HTTP GET and POST exchanges when logging into the authenticating web server directly, not through the security appliance. See the *Cisco Security Appliance Command Line Configuration Guide*, for more detail on extracting these parameters from the HTTP exchanges.

The following table describes the unique fields for configuring HTTP Form servers, for use with the [“Adding a Server to a Group” section on page 14-10](#).

| Field                      | Description                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start URL                  | The complete URL of the authenticating web server location where a pre-login cookie can be retrieved. This parameter must be configured only when the authenticating web server loads a pre-login cookie with the login page. A drop-down list offers both HTTP and HTTPS. The maximum number of characters is 1024, and there is no minimum.        |
| Action URI                 | The complete Uniform Resource Identifier for the authentication program on the authorizing web server. The maximum number of characters for the complete URI is 2048 characters.                                                                                                                                                                     |
| Username                   | The name of a username parameter—not a specific username—that must be submitted as part of the HTTP form used for SSO authentication. The maximum number of characters is 128, and there is no minimum.                                                                                                                                              |
| Password                   | The name of a user password parameter—not a specific password value—that must be submitted as part of the HTTP form used for SSO authentication. The maximum number of characters is 128, and there is no minimum.                                                                                                                                   |
| Hidden Values              | The hidden parameters for the HTTP POST request submitted to the authenticating web server for SSO authentication. This parameter is necessary only when it is expected by the authenticating web server as indicated by its presence in the HTTP POST request. The maximum number of characters is 2048.                                            |
| Authentication Cookie Name | (Optional) The name of the cookie that is set by the server on successful login and that contains the authentication information. It is used to assign a meaningful name to the authentication cookie to help distinguish it from other cookies that the web server may pass back. The maximum number of characters is 128, and there is no minimum. |

## Testing Server Authentication and Authorization

To determine whether the security appliance can contact an AAA server and authenticate or authorize a user, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups table, click the server group where the server resides.

The row is highlighted in the table.

**Step 2** From the Servers in the Selected Group table, click the server you want to test.

The row is highlighted in the table.

**Step 3** Click **Test**.

The Test AAA Server dialog box appears for that server.

**Step 4** Click the type of test you want to perform, **Authentication** or *Authorization*.

**Step 5** In the Username field, add a username.

**Step 6** If you are testing authentication, in the Password field, add the password for the username.

**Step 7** Click **OK**.

The security appliance sends an authentication or authorization test message to the server. If the test fails, ASDM displays an error message.

## Adding a User Account

The local database is used for the following features:

- ASDM per-user access

By default, you can log into ASDM with a blank username and the enable password (see [Device Name/Password, page 10-12](#)). However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.



**Note**

Although you can configure HTTP authentication using the local database, that functionality is always enabled by default. You should only configure HTTP authentication if you want to use a RADIUS or TACACS+ server for authentication.

- Console authentication
- Telnet and SSH authentication
- enable command authentication

This setting is for CLI-access only and does not affect the ASDM login.

- Command authorization

If you turn on command authorization using the local database, then the security appliance refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used. By default, all commands are either privilege level 0 or level 15. ASDM allows you to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels.

- Network access authentication
- VPN client authentication

You cannot use the local database for network access authorization.

For multiple context mode, you can configure usernames in the system execution space to provide individual logins at the CLI using the **login** command; however, you cannot configure any AAA rules that use the local database in the system execution space.

To add a user account to the security appliance local database, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Users/AAA > User Accounts pane, click **Add**. The Add User Account—Identity dialog box appears.
- Step 2** In the Username field, add a username between 4 to 64 characters long.
- Step 3** In the Password field add a password between 3 and 32 characters. Entries are case-sensitive. The field displays only asterisks. To protect security, we recommend a password length of at least 8 characters.
- Step 4** In the Confirm Password field, add the password again.  
For security purposes, only asterisks appear in the password fields.
- Step 5** To enable MSCHAP authentication, check **User authenticated using MSCHAP**.  
This option specifies that the password is converted to unicode and hashed using MD4 after you enter it. Use this feature if users are authenticated using MSCHAPv1 or MSCHAPv2.
- Step 6** To specify the VPN groups that the user belongs to, enter a group name in the Member of field, and click **Add**.  
To delete a VPN group, choose the group in the window, and click **Delete**.
- Step 7** In the Access Restriction area, set the management access level for a user. You must first enable management authorization using the **Perform authorization for exec shell access** option on the Configuration > Device Management > Users/AAA > AAA Access > Authorization tab.  
Choose one of the following options:
- **Full Access (ASDM, Telnet, SSH and console)**—If you configure authentication for management access using the local database (see the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 13-24](#)), then this option lets the user use ASDM, SSH, Telnet, and the console port. If you also configure enable authentication, then the user can access global configuration mode.
    - **Privilege Level**—Selects the privilege level for this user to use with local command authorization. The range is 0 (lowest) to 15 (highest). See the [“Configuring Local Command Authorization” section on page 13-29](#) for more information.
  - **CLI login prompt for SSH, Telnet and console (no ASDM access)**—If you configure authentication for management access using the local database (see the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 13-24](#)), then this option lets the user use SSH, Telnet, and the console port. The user cannot use ASDM for configuration (if you configure HTTP authentication). ASDM monitoring is allowed. If you also configure enable authentication, then the user cannot access global configuration mode.
  - **No ASDM, SSH, Telnet, or console access**—If you configure authentication for management access using the local database (see the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 13-24](#)), then this option disallows the user from accessing any management access method for which you configured authentication (excluding the Serial option; serial access is allowed).
- Step 8** If you want to configure VPN policy attributes for this user, see the [“Configuring VPN Policy Attributes for a User” section on page 14-19](#).
- Step 9** Click **Apply**.

The user is added to the local security appliance database and changes are saved to the running configuration.

**Note**

To configure the enable password from the User Accounts pane (instead of in [Device Name/Password, page 10-12](#)), change the password for the enable\_15 user. The enable\_15 user is always present in this pane, and represents the default username. This method of configuring the enable password is the only method available in ASDM for the system configuration. If you configured other enable level passwords at the CLI (**enable password 10**, for example), then those users are listed as enable\_10, etc.

## Configuring VPN Policy Attributes for a User

By default, each user inherits the settings set in the VPN policy. To override the settings, you can customize VPN attributes by performing the following steps:

**Step 1** If you have not already added a user according to the [“Adding a User Account” section on page 14-17](#), from the Configuration > Device Management > Users/AAA > User Accounts pane, click **Add**.

The Add User Account—Identity dialog box appears.

**Step 2** In the left-hand pane, click **VPN Policy**.

By default, the Inherit check box is checked for each option, which means the user account inherits the settings from the VPN policy. To override each setting, uncheck **Inherit**, and fill in a new value:

- Group Policy—Choose a group policy from the list.
- Tunneling Protocols—Specifies what tunneling protocols that this user can use, or whether to inherit the value from the group policy. Check the desired Tunneling Protocols check boxes to select the VPN tunneling protocols that this user can use. Users can use only the selected protocols. The choices are as follows:
  - IPSec—IP Security Protocol. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec.
  - Clientless SSL VPN—VPN via SSL/TLS. Uses a web browser to establish a secure remote-access tunnel to a VPN Concentrator; 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—Lets users connect after downloading the Cisco 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.
  - 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.

**Note**

If no protocol is selected, an error message appears.

- **Filter**—Specifies what filter 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 security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Configuration > VPN > VPN General > Group Policy pane.
- **Manage**—Displays the ACL Manager pane, on which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs).
- **Tunnel Group Lock**—Specifies whether to inherit the 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 user's assigned group. If it is not, the security appliance prevents the user from connecting. If the Inherit check box is not selected, the default value is --None--.
- **Store Password on Client System**—Specifies whether to inherit this setting from the group. Deselecting the Inherit check box activates the Yes and No radio buttons. Selecting Yes stores the login password on the client system (potentially a less-secure option). Selecting No (the default) requires the user to enter the password with each connection. For maximum security, we recommend that you *not do allow* password storage. This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.

**Step 3** To change Connection Settings, uncheck **Inherit**, and fill in a new value:

- **Access Hours**—If the Inherit check box is not selected, you can select 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 selected, the default value is --Unrestricted--.
- **New**—Opens the Add Time Range dialog box, on which you can specify a new set of access hours.
- **Simultaneous Logins**—If the Inherit check box is not selected, this 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.

- **Maximum Connect Time**—If the Inherit check box is not selected, this parameter specifies the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, select the Unlimited check box (the default).
- **Idle Timeout**—If the Inherit check box is not selected, this parameter specifies this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. This value does not apply to users of clientless SSL VPN connections.

**Step 4** To set a dedicated IP address for this user, enter an IP address and subnet mask in the Dedicated IP Address (Optional) area.

**Step 5** To configure clientless SSL settings, in the left-hand pane, click **Clientless SSL VPN**.

To override each setting, uncheck **Inherit**, and fill in a new value. See the “Group Policies” section on page 35-4.

**Step 6** To configure SSL VPN settings, in the left-hand pane, click **SSL VPN Client**.

To override each setting, uncheck **Inherit**, and fill in a new value. See the “Configuring SSL VPN Connections” section on page 35-34.



**Step 7** Click **Apply**.

---

## Configuring LDAP Attribute Maps

If you are introducing a security appliance to an existing LDAP directory, your existing LDAP attribute names and values are probably different from the existing ones. You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as needed. You can also show or clear attribute maps.



### Note

To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

The names of frequently mapped Cisco LDAP attributes and the type of user-defined attributes they would commonly be mapped to include:

*IETF-Radius-Class* – Department or user group  
*IETF-Radius-Filter-Id* – Access control list  
*IETF-Radius-Framed-IP-Address* – A static IP address  
*IPSec-Banner1* – A organization title  
*Tunneling-Protocols* – Allow or deny dial-in

For a list of Cisco LDAP attribute names and values, see [Appendix C, “Configuring an External LDAP Server”](#).

To map the LDAP attribute names used in your organization to their Cisco counterparts on the security appliance, perform the following steps:

- 
- Step 1** From the Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map pane, click **Add**.
- The Add LDAP Attribute Map dialog box appears with the Map Name tab active.
- Step 2** In the Name field, add a name for the map.
- Step 3** In the Customer Name field, add the name of your organization’s corresponding attribute.
- Step 4** From the Cisco Name drop-down list, choose an attribute.
- Step 5** Click **Add**.
- Step 6** To add more names, repeat steps 1 through 5.
- Step 7** To map the customer names, click the **Map Value** tab.
- Step 8** Click **Add**.
- The Add LDAP Attributes Map Value dialog box appears.
- Step 9** Choose the attribute from the Customer Name drop-down list.
- Step 10** In the Customer Value field, add the value for this attribute.
- Step 11** In the Cisco Value field, add the Cisco value that the value in step 10 maps to.
- Step 12** Click **Add**.
- The values are mapped.

- Step 13** To map more names, repeat steps 8 through 12.
- Step 14** Click **OK** to return to the Map Value tab, and then click **OK** again to close the dialog box.
- Step 15** In the LDAP Attribute Map pane, click **Apply**.  
The value mappings are saved in the running configuration.

## Adding an Authentication Prompt

You can specify text to display to the user during the AAA authentication challenge process. You can specify the AAA challenge text for HTTP, FTP, and Telnet access through the security appliance when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in.

If you do not specify an authentication prompt, users will see the following when authenticating with a RADIUS or TACACS+ server:

| Connection type | Default prompt      |
|-----------------|---------------------|
| FTP             | FTP authentication  |
| HTTP            | HTTP Authentication |
| Telnet          | None                |

To add an authentication prompt, perform the following steps:

- Step 1** From the Configuration > Device Management > Users/AAA > Authentication Prompt pane, add a message to appear above the username and password prompts that users see when logging in by entering text in the Prompt field.

The following are maximum characters allowed for authentication prompts:

| Application                 | Character limit for Authentication prompt |
|-----------------------------|-------------------------------------------|
| Microsoft Internet Explorer | 37                                        |
| Telnet                      | 235                                       |
| FTP                         | 235                                       |

- Step 2** In the Messages area, add messages in the User accepted message and User rejected message fields.
- If the user authentication occurs from Telnet, you can use the User accepted message and User rejected message options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the security appliance displays the User accepted message text, if specified, to the user; otherwise it displays the User rejected message text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The User accepted message and User rejected message text are not displayed.

- Step 3** Click **Apply**.

The changes are saved to the running configuration.

---





# CHAPTER 15

## High Availability

---

This section contains the following topics:

- [Understanding Failover, page 15-1](#)
- [Configuring Failover with the High Availability and Scalability Wizard, page 15-4](#)
- [Field Information for the Failover Panes, page 15-14](#)

## Understanding Failover

The Failover pane contains the settings for configuring failover on the security appliance. However, the Failover pane changes depending upon whether you are in multiple mode or single mode, and when you are in multiple mode, it changes based on the security context you are in.

Failover allows you to configure two security appliances so that one will take over operation if the other fails. Using a pair of security appliances, you can provide high availability with no operator intervention. The security appliance communicates failover information over a dedicated failover link. This failover link can be either a LAN-based connection or, on the PIX security appliance platform, a dedicated serial failover cable. The following information is communicated over the failover link:

- The failover state (active or standby).
- Hello messages (keep-alives).
- Network link status.
- MAC address exchange.
- Configuration replication.



### Caution

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

The security appliance supports two types of failover, Active/Standby and Active/Active. Additionally, failover can be stateful or stateless. For more information about the types of failover, see the following topics:

- [Active/Standby Failover, page 15-2](#)

- [Active/Active Failover, page 15-2](#)
- [Stateless \(Regular\) Failover, page 15-3](#)
- [Stateful Failover, page 15-3](#)

## Active/Standby Failover

In an Active/Standby configuration, the active security appliance handles all network traffic passing through the failover pair. The standby security appliance does not handle network traffic until a failure occurs on the active security appliance. Whenever the configuration of the active security appliance changes, it sends configuration information over the failover link to the standby security appliance.

When a failover occurs, the standby security appliance becomes the active unit. It assumes the IP and MAC addresses of the previously active unit. Because the other devices on the network do not see any changes in the IP or MAC addresses, ARP entries do not change or time out anywhere on the network.

Active/Standby failover is available to security appliances in single mode or multiple mode.

## Active/Active Failover

In an Active/Active failover configuration, both security appliances pass network traffic. Active/Active failover is only available to security appliances in multiple context mode.

To enable Active/Active failover on the security appliance, you need to create failover groups. If you enable failover without creating failover groups, you are enabling Active/Standby failover. A failover group is simply a logical group of one or more security contexts. You can create two failover groups on the security appliance. You should create the failover groups on the unit that will have failover group 1 in the active state. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.

As in Active/Standby failover, each unit in an Active/Active failover pair is given a primary or secondary designation. Unlike Active/Standby failover, this designation does not indicate which unit is active when both units start simultaneously. Each failover group in the configuration is given a primary or secondary role preference. This preference determines on which unit in the failover pair the contexts in the failover group appear in the active state when both units start simultaneously. You can have both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, balancing the traffic across the devices.

Initial configuration synchronization occurs when one or both units start. This synchronization occurs as follows:

- When both units start simultaneously, the configuration is synchronized from the primary unit to the secondary unit.
- When one unit starts while the other unit is already active, the unit that is starting up receives the configuration from the already active unit.

After both units are running, commands are replicated from one unit to the other as follows:

- Commands entered within a security context are replicated from the unit on which the security context appears in the active state to the peer unit.

**Note**

A context is considered in the active state on a unit if the failover group to which it belongs is in the active state on that unit.

- Commands entered in the system execution space are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state.
- Commands entered in the admin context are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state.

Failure to enter the commands on the appropriate unit for command replication to occur will cause the configurations to be out of synchronization. Those changes may be lost the next time the initial configuration synchronization occurs.

In an Active/Active failover configuration, failover occurs on a failover group basis, not a system basis. For example, if you designate both failover groups as active on the primary unit, and failover group 1 fails, failover group 2 remains active on the primary unit, while failover group 1 becomes active on the secondary unit.

**Note**

When configuring Active/Active failover, make sure that the combined traffic for both units is within the capacity of each unit.

## Stateless (Regular) Failover

Stateless failover is also referred to as regular failover. In stateless failover, all active connections are dropped when a failover occurs. Clients need to reestablish connections when the new active unit takes over.

## Stateful Failover

**Note**

Stateful Failover is not supported on the ASA 5505 series adaptive security appliance.

When Stateful Failover is enabled, the active unit in the failover pair continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

**Note**

The IP address and MAC address for the state and LAN failover links do not change at failover.

To use Stateful Failover, you must configure a state link to pass all state information to the standby unit. If you are using a LAN failover connection rather than the serial failover interface (available on the PIX security appliance platform only), you can use the same interface for the state link as the failover link. However, we recommend that you use a dedicated interface for passing state information the standby unit.

The following information is passed to the standby unit when Stateful Failover is enabled:

- NAT translation table.
- TCP connection table (except for HTTP), including the timeout connection.
- HTTP connection states (if HTTP replication is enabled).
- H.323, SIP, and MGCP UDP media connections.
- The system clock.

- The ISAKMP and IPsec SA table.

The following information is not copied to the standby unit when Stateful Failover is enabled:

- HTTP connection table (unless HTTP replication is enabled).
- The user authentication (uauth) table.
- The ARP table.
- Routing tables.

## Configuring Failover with the High Availability and Scalability Wizard

The High Availability and Scalability Wizard steps you through the process of creating an Active/Active failover configuration, and Active/Standby failover configuration, or a VPN Cluster Load Balancing configuration.

See the following topics for information about using the High Availability and Scalability Wizard:

- [Accessing and Using the High Availability and Scalability Wizard, page 15-4](#)
- [Configuring Active/Active Failover with the High Availability and Scalability Wizard, page 15-4](#)
- [Configuring Active/Standby Failover with the High Availability and Scalability Wizard, page 15-5](#)
- [Configuring VPN Load Balancing with the High Availability and Scalability Wizard, page 15-6](#)
- [Field Information for the High Availability and Scalability Wizard, page 15-7](#)

## Accessing and Using the High Availability and Scalability Wizard

To open the High Availability and Scalability Wizard, choose **Wizards > High Availability and Scalability Wizard** from the ASDM menu bar. The first screen of the wizard appears.

To move to the next screen of the wizard, click the **Next** button. You must complete the mandatory field of each screen before you can move to the next screen.

To move to a previous screen of the wizard, click the **Back** button. If information filled in on later screens of the wizard is not affected by the change you make to an earlier screen, that information remains on the screen as you move forward through the wizard again. You do not need to reenter it.

To leave the wizard at any time without saving any changes, click **Cancel**.

To send your configuration to the security appliance at the end of the wizard, click **Finish**.

## Configuring Active/Active Failover with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring Active/Active failover using the High Availability and Scalability Wizard. Each step in the procedure corresponds with a wizard screen. Click **Next** after completing each step, except for the last step, before moving to the next step. Each step also contains a reference to additional information that you may need to complete the step.

- 
- Step 1** Choose **Configure Active/Active** failover on the Choose the type of failover configuration screen.



- See [Choose the Type of Failover Configuration, page 15-7](#) for more information about this screen.
- Step 2** Enter the IP address of the failover peer on the Check Failover Peer Connectivity and Compatibility screen. Click **Test Compatibility**. You will not be able to move to the next screen until all compatibility tests are passed.
- See [Check Failover Peer Connectivity and Compatibility, page 15-8](#) for more information about this screen.
- Step 3** If the security appliance or the failover peer are in single context mode, change them to multiple context mode on the Change Device to Multiple Mode screen. When you change the security appliance to multiple context mode, it will reboot. ASDM automatically reestablishes communication with the security appliance when it has finished rebooting.
- See [Change Device to Multiple Mode, page 15-8](#) for more information about this screen.
- Step 4** (PIX 500 series security appliance only) Select cable-based or LAN-based failover on the Select Failover Communication Media screen.
- See [Select Failover Communication Media, page 15-9](#) for more information about this screen.
- Step 5** Assign security contexts to failover groups on the Context Configuration screen. You can add and delete contexts on this screen.
- See [Security Context Configuration, page 15-9](#) for more information about this screen.
- Step 6** Define the Failover Link on the Failover Link Configuration screen.
- See [Failover Link Configuration, page 15-10](#) for more information about this screen.
- Step 7** (Not available on the ASA 5505 security appliance) Define the Stateful Failover link on the State Link Configuration screen.
- See [State Link Configuration, page 15-11](#) for more information about this screen.
- Step 8** Add standby addresses to the security appliance interfaces on the Standby Address Configuration screen.
- See [Standby Address Configuration, page 15-11](#) for more information about this screen.
- Step 9** Review your configuration on the Summary screen. If necessary, use the Back button to go to a previous screen and make changes.
- See [Summary, page 15-14](#) for more information about this screen.
- Step 10** Click **Finish**.
- The failover configuration is sent to the security appliance and to the failover peer.
- 

## Configuring Active/Standby Failover with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring Active/Standby failover using the High Availability and Scalability Wizard. Each step in the procedure corresponds with a wizard screen. Click **Next** after completing each step, except for the last step, before moving to the next step. Each step also contains a reference to additional information that you may need to complete the step.

- Step 1** Choose **Configure Active/Standby** failover on the Choose the type of failover configuration screen. Click next.
- See [Choose the Type of Failover Configuration, page 15-7](#) for more information about this screen.

- Step 2** Enter the IP address of the failover peer on the Check Failover Peer Connectivity and Compatibility screen. Click **Test Compatibility**. You will not be able to move to the next screen until all compatibility tests are passed.
- See [Check Failover Peer Connectivity and Compatibility, page 15-8](#) for more information about this screen.
- Step 3** (PIX 500 series security appliance only) Select cable-based or LAN-based failover on the Select Failover Communication Media screen.
- See [Select Failover Communication Media, page 15-9](#) for more information about this screen.
- Step 4** Define the Failover Link on the Failover Link Configuration screen.
- See [Failover Link Configuration, page 15-10](#) for more information about this screen.
- Step 5** (Not available on the ASA 5505 security appliance) Define the Stateful Failover link on the State Link Configuration screen.
- See [State Link Configuration, page 15-11](#) for more information about this screen.
- Step 6** Add standby addresses to the security appliance interfaces on the Standby Address Configuration screen.
- See [Standby Address Configuration, page 15-11](#) for more information about this screen.
- Step 7** Review your configuration on the Summary screen. If necessary, use the Back button to go to a previous screen and make changes.
- See [Summary, page 15-14](#) for more information about this screen.
- Step 8** Click **Finish**.
- The failover configuration is sent to the security appliance and to the failover peer.
- 

## Configuring VPN Load Balancing with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring VPN cluster load balancing using the High Availability and Scalability Wizard. Each step in the procedure corresponds with a wizard screen. Click **Next** after completing each step, except for the last step, before moving to the next step. Each step also contains a reference to additional information that you may need to complete the step.

- Step 1** Choose **Configure VPN Cluster Load Balancing** failover on the Choose the type of failover configuration screen.
- See [Choose the Type of Failover Configuration, page 15-7](#) for more information about this screen.
- Step 2** Configure the VPN load balancing settings on the VPN Cluster Load Balancing Configuration screen.
- See [VPN Cluster Load Balancing Configuration, page 15-12](#) for more information about this screen.
- Step 3** Review your configuration on the Summary screen. If necessary, use the Back button to go to a previous screen and make changes.
- See [Summary, page 15-14](#) for more information about this screen.
- Step 4** Click **Finish**.
- The failover configuration is sent to the security appliance and to the failover peer.
-

## Field Information for the High Availability and Scalability Wizard

The following dialogs are available in the High Availability and Scalability Wizard. You will not see every dialog box when you run through the wizard; each dialog box appears depending on the type of failover you are configuring and the hardware platform you are configuring it on.

- [Choose the Type of Failover Configuration, page 15-7](#)
- [Check Failover Peer Connectivity and Compatibility, page 15-8](#)
- [Change Device to Multiple Mode, page 15-8](#)
- [Security Context Configuration, page 15-9](#)
- [Failover Link Configuration, page 15-10](#)
- [State Link Configuration, page 15-11](#)
- [Standby Address Configuration, page 15-11](#)
- [VPN Cluster Load Balancing Configuration, page 15-12](#)
- [Summary, page 15-14](#)

### Choose the Type of Failover Configuration

The Choose the Type of Failover Configuration screen lets you select the type of failover to configure.

#### Fields

The Choose the Type of Failover Configuration displays the following informational fields. These are useful for determining the failover capabilities of the security appliance.

- **Hardware Model**—(*Display only*) Displays the security appliance model number.
- **No. of Interfaces**—(*Display only*) Displays the number of interfaces available on the security appliance.
- **No. of Modules**—(*Display only*) Displays the number of modules installed on the security appliance.
- **Software Version**—(*Display only*) Displays the version of the platform software on the security appliance.
- **Failover License**—(*Display only*) Displays the type of failover license installed on the device. You may need to purchase an upgraded license to configure failover.
- **Firewall Mode**—(*Display only*) Displays the firewall mode (routed or transparent) and the context mode (single or multiple).

Choose the type of failover configuration you are configuring:

- **Configure Active/Active Failover**—Configures the security appliance for Active/Active failover.
- **Configure Active/Standby Failover**—Configures the security appliance for Active/Standby failover.
- **Configure VPN Cluster Load Balancing**—Configures the security appliance to participate in VPN load balancing as part of a cluster.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Check Failover Peer Connectivity and Compatibility

The Check Failover Peer Connectivity and Compatibility screen lets you verify that the selected failover peer is reachable and compatible with the current unit. If any of the connectivity and compatibility tests fail, you must correct the problem before you can proceed with the wizard.

### Fields

- Peer IP Address—Enter the IP address of the peer unit. This address does not have to be the failover link address, but it must be an interface that has ASDM access enabled on it.
- Test Compatibility—Click this button to perform the following connectivity and compatibility tests:
  - Connectivity test from this ASDM to the peer unit
  - Connectivity test from this firewall device to the peer firewall device
  - Hardware compatibility test
  - Software version compatibility
  - Failover license compatibility
  - Firewall mode compatibility

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Change Device to Multiple Mode

The Change Device to Multiple Mode dialog box appears for Active/Active failover configuration only. Active/Active failover requires the security appliance to be in multiple context mode. This dialog box lets you convert a security appliance in single context mode to multiple context mode.

When you convert from single context mode to multiple context mode, the security appliance creates the system configuration and the admin context from the current running configuration. The admin context configuration is stored in the admin.cfg file. The conversion process does not save the previous startup configuration, so if the startup configuration differed from the running configuration, those differences are lost.

Converting the security appliance from single context mode to multiple context mode causes the security appliance to reboot. However the High Availability and Scalability Wizard restores connectivity with the newly created admin context and reports the status in the Devices Status field in this dialog box.

You need to convert both the current security appliance and the peer security appliance to multiple context mode before you can proceed.

#### Fields

- Change *device* To Multiple Context—Causes the security appliance to change to multiple context mode. *device* is the hostname of the security appliance.
- Change *device* (peer) To Multiple Context—Causes the peer unit to change to multiple context mode. *device* is the hostname of the security appliance.
- Device Status—(*Display only*) Displays the status of the security appliance while converting to multiple context mode.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Select Failover Communication Media

The Select Failover Communication Media appears only on PIX 500 series security appliances. This screen lets you select between using a failover cable or LAN-based connection for the failover link.

#### Fields

- Use Failover Cable—Choose this option to use a dedicated failover cable for failover communication.
- Use LAN-based connection—Choose this option to use a network connection for failover communication.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Security Context Configuration

The Security Context Configuration screen appears for Active/Active configuration only. The Security Context Configuration screen lets you assign security contexts to failover groups. It displays the security contexts currently configured on the device and lets you add new ones or remove existing ones as needed.

Although you can create security contexts on this screen, you cannot assign interfaces to those contexts or configure any other properties for them. To configure context properties and assign interfaces to a context, you need to use the System > Security Contexts pane.

#### Fields

- **Name**—Displays the name of the security context. To change the name, click the name and type a new name.
- **Failover Group**—Displays the failover group the context is assigned to. To change the failover group for a security context, click the failover group and select the new failover group number from the drop-down list.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Failover Link Configuration

The Failover Link Configuration screen only appears if you are configuring LAN-based failover; it does not appear if you are configuring a PIX 500 series security appliance for cable-based failover.

#### Fields

- **LAN Interface**—Choose the interface to use for failover communication from the drop-down list.
- **Logical Name**—Type a name for the interface.
- **Active IP**—Type the IP address used for the failover link on the unit that has failover group 1 in the active state.
- **Standby IP**—Type the IP address used for the failover link on the unit that has failover group 1 in the standby state.
- **Subnet Mask**—Type or select a subnet mask for the Active IP and Standby IP addresses.
- **Secret Key**—(Optional) Enter the key used to encrypt failover communication. If this field is left blank, failover communication, including any passwords or keys in the configuration sent during command replication, is in clear text.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## State Link Configuration

The State Link Configuration screen does not appear in the wizard for ASDM running on the ASA 5505 platform.

The State Link Configuration lets you enable Stateful Failover and configure the Stateful Failover link properties.

### Fields

- Use the LAN link as the State Link—Choose this option to pass state information across the LAN-based failover link. This option is not available on PIX 500 series security appliances configured for cable-based failover.
- Disable Stateful Failover—Choose this option to disable Stateful Failover.
- Configure another interface for Stateful failover—Choose this option to configure an unused interface as the Stateful Failover interface.
  - State Interface—Choose the interface you want to use for Stateful Failover communication from the drop-down list.
  - Logical Name—Type the name for the Stateful Failover interface.
  - Active IP—Type the IP address for the Stateful Failover link on the unit that has failover group 1 in the active state.
  - Standby IP—Type the IP address for the Stateful Failover link on the unit that has failover group 1 in the standby state.
  - Subnet Mask—Type or select a subnet mask for the Active IP and Standby IP addresses.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Standby Address Configuration

Use the Standby Address Configuration screen to assign standby addresses to the interface on the security appliance.

### Fields

- Device/Interface—(Active/Standby failover) Displays the interfaces configured on the failover units. Click the plus sign (+) by a device name to displays the interfaces on that device. Click the minus sign (-) by a device name to hides the interfaces on that device.
- Device/Group/Context/Interface—(Active/Active failover) Displays the interfaces configured on the failover unit. The interfaces are grouped by context and the contexts are grouped by failover group. Click the plus sign (+) by a device, failover group, or context name to expand the list. Click the minus sign (-) by a device, failover group, or context name to collapse the list.

- **Active IP**—Double-click this field to edit or add an active IP address. Changes to this field also appear in the Standby IP field for the corresponding interface on the peer unit.
- **Standby IP**—Double-click this field to edit or add a standby IP address. Changes to this field also appear in the Active IP field for the corresponding interface on the peer unit.
- **Is Monitored**—Check this check box to enable health monitoring for that interface. Uncheck the check box to disable the health monitoring. By default, health monitoring of physical interfaces is enabled and health monitoring of virtual interfaces is disabled.
- **ASR Group**—Select the asynchronous group ID from the drop-down list. This setting is only available for physical interface. For virtual interfaces this field displays “None”.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## VPN Cluster Load Balancing Configuration

If you have a remote-client configuration in which you are using two or more security appliances connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called *load balancing*. 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 and availability.

Use the VPN Cluster Load Balancing Configuration screen to set parameters necessary for this device to participate in a load balancing cluster.



### Note

To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or 5540. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Enabling load balancing involves:

- Configuring the load-balancing cluster by establishing a common virtual cluster IP address, UDP port (if necessary), and IPsec shared secret for the cluster. These values are identical for every device in the cluster.
- Configuring the participating device by enabling load balancing on the device and defining device-specific properties. These values vary from device to device.



**Note**

Load balancing is effective only on remote sessions initiated with the Cisco VPN Client (Release 3.0 and later), the Cisco VPN 3002 Hardware Client (Release 3.5 and later), or the ASA 5505 operating as an Easy VPN Client. All other clients, including LAN-to-LAN connections, can connect to a security appliance on which load balancing is enabled, but the cannot participate in load balancing.

To implement load balancing, you group together logically two or more devices on the same private LAN-to-LAN network into a *virtual cluster*.

**Fields**

- **Cluster IP Address**—Specifies the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the security appliances in the virtual cluster.
- **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.
- **Enable IPsec Encryption**—Enables or disables IPsec encryption. If you select this check box, you must also specify and verify a shared secret. The security appliances 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, select this check box.

**Note**

When using encryption, you must have previously configured the load-balancing inside interface. If that interface is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.

If the load-balancing inside interface is enabled when you configured cluster encryption, but is disabled before you configure the participation of the device in the virtual cluster, you get an error message when you select the Participate in Load Balancing Cluster check box, and encryption is not enabled for the cluster.

- **Shared Secret Key**—Specifies the shared secret to between IPsec peers when you enable IPsec encryption. The value you enter in the box appears as consecutive asterisk characters.
- **Priority Of This Device**—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 secondary 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.

- **Public Interface Of This Device**—Specifies the name or IP address of the public interface for this device.

- Private Interface Of This Device—Specifies the name or IP address of the private interface for this device.
- 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Summary

The Summary screen displays the results of the configuration steps you performed in the previous wizard panels.

### Fields

The configuration appears in the center of the screen. Verify your settings and click **Finish** to send your configuration to the device. If you are configuring failover, the configuration is also sent to the failover peer. If you need to change a setting, click **Back** until you reach the screen where you need to make the change. Make the change and click **Next** until you return to the Summary screen.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | •      |

## Field Information for the Failover Panes

What displays on the failover pane depends upon the mode you are in (single or multiple context mode) and whether you are in the system execution space or in a security context.

This section contains the following topics:

- [Failover - Single Mode](#)
- [Failover-Multiple Mode, Security Context](#)
- [Failover-Multiple Mode, System](#)

## Failover - Single Mode

The Failover pane contains the tabs where you can configure Active/Standby failover in single context mode. For more information about failover, see [Understanding Failover](#). For more information about configuring the settings on each tab of the Failover pane, see the following information. Note that the Interfaces tabs changes based on whether you are in routed firewall mode or transparent firewall mode.

- [Failover: Setup](#)
- [Failover: Interfaces \(Routed Firewall Mode\)](#)
- [Failover: Interfaces \(Transparent Firewall Mode\)](#)
- [Failover: Criteria](#)
- [Failover: MAC Addresses](#)

### Failover: Setup

Use this tab to enable failover on the security appliance. You also designate the failover link and the state link, if using Stateful Failover, on this tab.

For more information about configuring failover in general, see [Understanding Failover](#).

#### Fields

- **Enable Failover**—Checking this check box enables failover and lets you configure a standby security appliance.



#### Note

The speed and duplex settings for the failover interface cannot be changed when Failover is enabled. To change these settings for the failover interface, you must configure them in the Configuration > Interfaces pane before enabling failover.

ASDM displays a dialog box asking if you want to configure the peer unit when you enable failover. This dialog box also appears when the Preferred Role setting or, on the PIX security appliance platform, the Enable LAN rather than serial cable failover setting changes.

- **Peer IP Address**—Enter an IP address on the peer unit that ASDM can connect to. This field appears on the Do you want to configure the failover peer firewall dialog box.
- **Use 32 hexadecimal character key**—Check this check box to enter a hexadecimal value for the encryption key in the Shared Key box. Uncheck this check box to enter an alphanumeric shared secret in the Shared Key box.
- **Shared Key**—Specifies the failover shared secret or key for encrypted and authenticated communications between failover pairs.

If you checked the Use 32 hexadecimal character key check box, then enter a hexadecimal encryption key. The key must be 32 hexadecimal characters (0-9, a-f).

If you unchecked the Use 32 hexadecimal character key check box, then enter an alphanumeric shared secret. The shared secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

- **Enable LAN rather than serial cable failover**—(PIX security appliance platform only) Check this check box to enable LAN Failover. Uncheck this check box to use the dedicated serial cable as the failover link.
- **LAN Failover**—Contains the fields for configuring LAN Failover.

- Interface—Specifies the interface used for failover communication. Failover requires a dedicated interface, however you can share the interface with Stateful Failover.  
Only unconfigured interfaces or subinterfaces are displayed in this list and can be selected as the LAN Failover interface. Once you specify an interface as the LAN Failover interface, you cannot edit that interface in the Configuration > Interfaces pane.
- Active IP—Specifies the IP address for the failover interface on the active unit.
- Subnet Mask—Specifies the mask for the failover interface on the primary and secondary unit.
- Logical Name—Specifies the logical name of the interface used for failover communication.
- Standby IP—Specifies the IP address used by the secondary unit to communicate with the primary unit
- Preferred Role—Specifies whether the preferred role for this security appliance is as the primary or secondary unit in a LAN failover.
- State Failover—Contains the fields for configuring Stateful Failover.

**Note**

Stateful Failover is not available on the ASA 5505 platform. This area does not appear on ASDM running on an ASA 5505 security appliance.

- Interface—Specifies the interface used for state communication. You can choose an unconfigured interface or subinterface, the LAN Failover interface, or the Use Named option.

**Note**

We recommend that you use two separate, dedicated interfaces for the LAN Failover interface and the Stateful Failover interface.

If you choose an unconfigured interface or subinterface, you must supply the Active IP, Subnet Mask, Standby IP, and Logical Name for the interface.

If you choose the LAN Failover interface, you do not need to specify the Active IP, Subnet Mask, Logical Name, and Standby IP values; the values specified for the LAN Failover interface are used.

If you choose the Use Named option, the Logical Name field becomes a drop-down list of named interfaces. Choose the interface from this list. The Active IP, Subnet Mask, and Standby IP values do not need to be specified. The values specified for the interface are used. Be sure to specify a standby IP address for the selected interface on the Interfaces tab.

**Note**

Because Stateful Failover can generate a large amount of traffic, performance for both Stateful Failover and regular traffic can suffer when you use a named interface.

- Active IP—Specifies the IP address for the Stateful Failover interface on the primary unit. This field is dimmed if the LAN Failover interface or Use Named option is selected in the Interface drop-down list.
- Subnet Mask—Specifies the mask for the Stateful Failover interfaces on the primary and secondary units. This field is dimmed if the LAN Failover interface or Use Named option is selected in the Interface drop-down list.

- Logical Name—Specifies the logical interface used for failover communication. If you selected the Use Named option in the Interface drop-down list, this field displays a list of named interfaces. This field is dimmed if the LAN Failover interface is selected in the Interface drop-down list.
- Standby IP—Specifies the IP address used by the secondary unit to communicate with the primary unit. This field is dimmed if the LAN Failover interface or Use Named option is selected in the Interface drop-down list.
- Enable HTTP replication—Selecting this check box enables Stateful Failover to copy active HTTP sessions to the standby firewall. If you do not allow HTTP replication, then HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover: Interfaces (Routed Firewall Mode)

Use this tab to define the standby IP address for each interface on the security appliance and to specify whether the status of the interface should be monitored.

For more information about configuring failover in general, see [Understanding Failover](#).

### Fields

- Interface—Lists the interfaces on the security appliance and identifies their active IP address, standby IP address, and monitoring status.
  - Interface Name column—Identifies the interface name.
  - Active IP column—Identifies the active IP address for this interface.
  - Standby IP column—Identifies the IP address of the corresponding interface on the standby failover unit.
  - Is Monitored column—Specifies whether this interface is monitored for failure.
- Edit—Displays the [Edit Failover Interface Configuration \(Routed Firewall Mode\)](#) dialog box for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

For more information about failover in general, see [Understanding Failover](#).

**Edit Failover Interface Configuration (Routed Firewall Mode)**

Use the Edit Failover Interface Configuration dialog box to define the standby IP address for an interface and to specify whether the status of the interface should be monitored.

**Fields**

- Interface Name—Identifies the interface name.
- Active IP Address—Identifies the IP address for this interface. This field does not appear if an IP address has not been assigned to the interface.
- Subnet Mask—Identifies the mask for this interface. This field does not appear if an IP address has not been assigned to the interface.
- Standby IP Address—Specifies the IP address of the corresponding interface on the standby failover unit. This field does not appear if an IP address has not been assigned to the interface.
- Monitor interface for failure—Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Monitored failover interfaces can have the following status:
  - Unknown—Initial status. This status can also mean the status cannot be determined.
  - Normal—The interface is receiving traffic.
  - Testing—Hello messages are not heard on the interface for five poll times.
  - Link Down—The interface is administratively down.
  - No Link—The physical link for the interface is down.
  - Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**For More Information**

For more information about failover in general, see [Understanding Failover](#).

## Failover: Interfaces (Transparent Firewall Mode)

Use this tab to define the standby management IP address and to specify whether the status of the interfaces on the security appliance should be monitored.

### Fields

- Interface—Lists the interfaces on the security appliance and identifies their monitoring status.
  - Interface Name column—Identifies the interface name.
  - Is Monitored column—Specifies whether this interface is monitored for failure.
- Edit—Displays the [Edit Failover Interface Configuration \(Transparent Firewall Mode\)](#) dialog box for the selected interface.
- Management IP Address—Identifies the active and standby management IP addresses for the security appliance or for a context in transparent firewall mode.
  - Active—Identifies the active management IP address.
  - Standby—Specifies the management IP address on the standby failover unit.
- Management Netmask—Identifies the mask associated with the active and standby management IP addresses.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | —        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Edit Failover Interface Configuration (Transparent Firewall Mode)

Use the Edit Failover Interface Configuration dialog box to specify whether the status of the interface should be monitored.

### Fields

- Interface Name—Identifies the interface name.
- Monitor interface for failure—Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. Monitored failover interfaces can have the following status:
  - Unknown—Initial status. This status can also mean the status cannot be determined.
  - Normal—The interface is receiving traffic.
  - Testing—Hello messages are not heard on the interface for five poll times.
  - Link Down—The interface is administratively down.

- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | —        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover: Criteria

Use this tab to define criteria for failover, such as how many interfaces must fail and how long to wait between polls. The hold time specifies the interval to wait without receiving a response to a poll before unit failover.

### Fields

- Interface Policy—Contains the fields for defining the policy for failover when monitoring detects an interface failure.
  - Number of failed interfaces that triggers failover—When the number of failed monitored interfaces exceeds the value you set with this command, then the security appliance fails over. The range is between 1 and 250 failures.
  - Percentage of failed interfaces that triggers failover—When the number of failed monitored interfaces exceeds the percentage you set with this command, then the security appliance fails over.
- Failover Poll Times—Contains the fields for defining how often hello messages are sent on the failover link, and, optionally, how long to wait before testing the peer for failure if no hello messages are received.
  - Unit Failover—The amount of time between hello messages among units. The range is between 1 and 15 seconds or between 200 and 999 milliseconds.
  - Unit Hold Time—Sets the time during which a unit must receive a hello message on the failover link, or else the unit begins the testing process for peer failure. The range is between 1 and 45 seconds or between 800 and 999 milliseconds. You cannot enter a value that is less than 3 times the polltime.
  - Monitored Interfaces—The amount of time between polls among interfaces. The range is between 1 and 15 seconds or 500 to 999 milliseconds.
  - Interface Hold Time—Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 seconds.



### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover: MAC Addresses

The MAC Addresses tab lets you configure the virtual MAC addresses for the interfaces in an Active/Standby failover pair.



#### Note

This tab is not available on the ASA 5505 platform.

In Active/Standby failover, the MAC addresses for the primary unit are always associated with the active IP addresses. If the secondary unit boots first and becomes active, it uses the burned-in MAC address for its interfaces. When the primary unit comes online, the secondary unit obtains the MAC addresses from the primary unit. The change can disrupt network traffic.

You can configure virtual MAC addresses for each interface to ensure that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit. If you do not specify virtual MAC addresses, then the failover pair uses the burned-in NIC address as the MAC address.



#### Note

You cannot configure a virtual MAC address for the failover or state links. The MAC and IP addresses for those links do not change during failover.

### Fields

- **MAC Addresses**—Lists physical interfaces on the security appliance for which an active and standby virtual MAC address has been configured.
  - **Physical Interface column**—Identifies the physical interface for which failover virtual MAC addresses are configured.
  - **Active MAC Address column**—Identifies the MAC address of the active security appliance (usually primary).
  - **Standby MAC Address column**—Identifies the MAC address of the standby security appliance (usually secondary).
- **Add**—Displays the Add Interface MAC Address dialog box. You cannot assign virtual MAC addresses to the LAN failover and Stateful Failover interfaces. See [Add/Edit Interface MAC Address](#) for more information.
- **Edit**—Displays the Edit Interface MAC Address dialog box for the selected interface. See [Add/Edit Interface MAC Address](#) for more information.

- **Delete**—Removes the currently selected interface from the MAC addresses table. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Add/Edit Interface MAC Address

Use the Add/Edit Interface MAC Address dialog box to define the active and standby virtual MAC addresses for an interface.

### Fields

- **Physical Interface**—Specifies the physical interface for which you are defining failover virtual MAC addresses. Because the MAC addresses do not change for the LAN failover and Stateful Failover interfaces during failover, you cannot choose these interfaces.
- **MAC Addresses**—Contains the fields for specifying the active and standby virtual MAC addresses for the interface.
  - **Active Interface**—Specifies the MAC address of the interface on the active security appliance (usually primary). Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).
  - **Standby Interface**—Specifies the MAC address of the interface on the standby security appliance (usually secondary). Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover-Multiple Mode, Security Context

The fields displayed on the Failover pane in multiple context mode change depending upon whether the context is in transparent or routed firewall mode.

This section contains the following topics:

- [Failover - Routed](#)
- [Failover - Transparent](#)

### Failover - Routed

Use this pane to define the standby IP address for each interface in the security context and to specify whether the status of the interface should be monitored.

#### Fields

- Interface table—Lists the interfaces on the security appliance and identifies their active IP address, standby IP address, and monitoring status.
  - Interface Name column—Identifies the interface name.
  - Active IP column—Identifies the active IP address for this interface.
  - Standby IP column—Identifies the IP address of the corresponding interface on the standby failover unit.
  - Is Monitored column—Specifies whether this interface is monitored for failure.
- Edit—Displays the [Edit Failover Interface Configuration](#) dialog box for the selected interface.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | —                | •        | —      |

#### For More Information

For more information about failover in general, see [Understanding Failover](#).

### Edit Failover Interface Configuration

Use the Edit Failover Interface Configuration dialog box to define the standby IP address for an interface and to specify whether the status of the interface should be monitored.

#### Fields

- Interface Name—Identifies the interface name.
- Active IP Address—Identifies the IP address for this interface. This field does not appear if an IP address has not been assigned to the interface.

- Subnet Mask—Identifies the mask for this interface. This field does not appear if an IP address has not been assigned to the interface.
- Standby IP Address—Specifies the IP address of the corresponding interface on the standby failover unit. This field does not appear if an IP address has not been assigned to the interface.
- Monitor interface for failure—Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. Monitored failover interfaces can have the following status:
  - Unknown—Initial status. This status can also mean the status cannot be determined.
  - Normal—The interface is receiving traffic.
  - Testing—Hello messages are not heard on the interface for five poll times.
  - Link Down—The interface is administratively down.
  - No Link—The physical link for the interface is down.
  - Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | —                | •        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover - Transparent

Use this pane to define the standby IP address for the management interface for the security context and to specify whether the status of the interfaces on the security context should be monitored.

### Fields

- Interface—Lists the interfaces for the security context and identifies their monitoring status.
  - Interface Name—Identifies the interface name.
  - Is Monitored—Specifies whether this interface is monitored for failure.
- Edit—Displays the [Edit Failover Interface Configuration](#) dialog box for the selected interface.
- Management IP Address—Identifies the active and standby management IP addresses for the security context.
  - Active—Identifies the management IP address for the active failover unit.
  - Standby—Specifies the management IP address for the standby failover unit.
- Management Netmask—Identifies the mask associated with the management address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | —                | •        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Edit Failover Interface Configuration

Use the Edit Failover Interface Configuration dialog box to specify whether the status of the interface should be monitored.

### Fields

- Interface Name—Identifies the interface name.
- Monitor interface for failure—Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. Monitored failover interfaces can have the following status:
  - Unknown—Initial status. This status can also mean the status cannot be determined.
  - Normal—The interface is receiving traffic.
  - Testing—Hello messages are not heard on the interface for five poll times.
  - Link Down—The interface is administratively down.
  - No Link—The physical link for the interface is down.
  - Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | —                | •        | —      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover-Multiple Mode, System

This pane includes tabs for configuring the system-level failover settings in the system context of a security appliance in multiple context mode. In multiple mode, you can configure Active/Standby or Active/Active failover. Active/Active failover is automatically enabled when you create failover groups in the device manager. For both types of failover, you need to provide system-level failover settings in the system context, and context-level failover settings in the individual security contexts. For more information about configuring failover in general, see [Understanding Failover](#).

See the following topics for more information:

- [Failover > Setup Tab](#)
- [Failover > Criteria Tab](#)
- [Failover > Active/Active Tab](#)
- [Failover > MAC Addresses Tab](#)

### Failover > Setup Tab

Use this tab to enable failover on a security appliance in multiple context mode. You also designate the failover link and the state link, if using Stateful Failover, on this tab.

#### Fields

- **Enable Failover**—Checking this check box enables failover and lets you configure a standby security appliance.



#### Note

The speed and duplex settings for an interface cannot be changed when Failover is enabled. To change these settings for the failover interface, you must configure them in the Configuration > Interfaces pane before enabling failover.

- **Use 32 hexadecimal character key**—Check this check box to enter a hexadecimal value for the encryption key in the Shared Key field. Uncheck this check box to enter an alphanumeric shared secret in the Shared Key field.
- **Shared Key**—Specifies the failover shared secret or key for encrypted and authenticated communications between failover pairs.

If you checked the Use 32 hexadecimal character key check box, then enter a hexadecimal encryption key. The key must be 32 hexadecimal characters (0-9, a-f).

If you cleared the Use 32 hexadecimal character key check box, then enter an alphanumeric shared secret. The shared secret can be from 1 to 63 characters. Valid characters are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

- **Enable LAN rather than serial cable failover**—(PIX security appliance platform only) Check this check box to enable LAN failover. Uncheck this check box to use the dedicated serial link as the failover link.
- **LAN Failover**—Contains the fields for configuring LAN Failover.
  - **Interface**—Specifies the interface used for failover communication. Failover requires a dedicated interface, however, you can use the same interface for Stateful Failover.

Only unconfigured interfaces or subinterfaces that have not been assigned to a context are displayed in this list and can be selected as the LAN Failover interface. Once you specify an interface as the LAN Failover interface, you cannot edit that interface in the Configuration > Interfaces pane or assign that interface to a context.

- Active IP—Specifies the IP address for the failover interface on the active unit.
- Subnet Mask—Specifies the mask for the failover interface on the active unit.
- Logical Name—Specifies the logical name for the failover interface.
- Standby IP—Specifies the IP address of the standby unit.
- Preferred Role—Specifies whether the preferred role for this security appliance is as the primary or secondary unit in a LAN failover.
- State Failover—Contains the fields for configuring Stateful Failover.
  - Interface—Specifies the interface used for failover communication. You can choose an unconfigured interface or subinterface or the LAN Failover interface.

If you choose the LAN Failover interface, the interface needs enough capacity to handle both the LAN Failover and Stateful Failover traffic. Also, you do not need to specify the Active IP, Subnet Mask, Logical Name, and Standby IP values; the values specified for the LAN Failover interface are used.



**Note** We recommend that you use two separate, dedicated interfaces for the LAN Failover interface and the Stateful Failover interface.

- Active IP—Specifies the IP address for the Stateful Failover interface on the active unit.
- Subnet Mask—Specifies the mask for the Stateful Failover interface on the active unit.
- Logical Name—Specifies the logical name for the Stateful Failover interface.
- Standby IP—Specifies the IP address of the standby unit.
- Enable HTTP replication—Checking this check box enables Stateful Failover to copy active HTTP sessions to the standby firewall. If you do not allow HTTP replication, then HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover > Criteria Tab

Use this tab to define criteria for failover, such as how many interfaces must fail and how long to wait between polls. The hold time specifies the interval to wait without receiving a response to a poll before unit failover.



### Note

If you are configuring Active/Active failover, you do not use this tab to define the interface policy; instead, you define the interface policy for each failover group using the [Failover > Active/Active Tab](#). With Active/Active failover, the interface policy settings defined for each failover group override the settings on this tab. If you disable Active/Active failover, then the settings on this tab are used.

### Fields

- **Interface Policy**—Contains the fields for defining the policy for failover when monitoring detects an interface failure.
  - **Number of failed interfaces that triggers failover**—When the number of failed monitored interfaces exceeds the value you set with this command, then the security appliance fails over. The range is between 1 and 250 failures.
  - **Percentage of failed interfaces that triggers failover**—When the number of failed monitored interfaces exceeds the percentage you set with this command, then the security appliance fails over.
- **Failover Poll Times**—Contains the fields for defining how often hello messages are sent on the failover link, and, optionally, how long to wait before testing the peer for failure if no hello messages are received.
  - **Unit Failover**—The amount of time between hello messages among units. The range is between 1 and 15 seconds or between 200 and 999 milliseconds.
  - **Unit Hold Time**—Sets the time during which a unit must receive a hello message on the failover link, or else the unit begins the testing process for peer failure. The range is between 1 and 45 seconds or between 800 and 999 milliseconds. You cannot enter a value that is less than 3 times the polltime.
  - **Monitored Interfaces**—The amount of time between polls among interfaces. The range is between 1 and 15 seconds or 500 to 999 milliseconds.
  - **Interface Hold Time**—Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 seconds.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).



## Failover > Active/Active Tab

Use this tab to enable Active/Active failover on the security appliance by defining failover groups. In an Active/Active failover configuration, both security appliances pass network traffic. Active/Active failover is only available to security appliances in multiple mode.

A failover group is simply a logical group of security contexts. You can create two failover groups on the security appliance. You must create the failover groups on the active unit in the failover pair. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.



### Note

When configuring Active/Active failover, make sure that the combined traffic for both units is within the capacity of each unit.

### Fields

- Failover Groups—Lists the failover groups currently defined on the security appliance.
  - Group Number—Specifies the failover group number. This number is used when assigning contexts to failover groups.
  - Preferred Role—Specifies the unit in the failover pair, primary or secondary, on which the failover group appears in the active state when both units start up simultaneously or when the preempt option is specified. You can have both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, balancing the traffic across the devices.
  - Preempt Enabled—Specifies whether the unit that is the preferred failover device for this failover group should become the active unit after rebooting.
  - Preempt Delay—Specifies the number of seconds that the preferred failover device should wait after rebooting before taking over as the active unit for this failover group. The range is between 0 and 1200 seconds.
  - Interface Policy—Specifies either the number of monitored interface failures or the percentage of failures that are allowed before the group fails over. The range is between 1 and 250 failures or 1 and 100 percent.
  - Interface Poll Time—Specifies the amount of time between polls among interfaces. The range is between 1 and 15 seconds.
  - Replicate HTTP—Identifies whether Stateful Failover should copy active HTTP sessions to the standby firewall for this failover group. If you do not allow HTTP replication, then HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link. This setting overrides the HTTP replication setting on the Setup tab.
- Add—Displays the Add Failover Group dialog box. This button is only enabled if less than 2 failover groups exist. See [Add/Edit Failover Group](#) for more information.
- Edit—Displays the Edit Failover Group dialog box for the selected failover group. See [Add/Edit Failover Group](#) for more information.
- Delete—Removes the currently selected failover group from the failover groups table. This button is only enabled if the last failover group in the list is selected.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

**For More Information**

For more information about failover in general, see [Understanding Failover](#).

**Add/Edit Failover Group**

Use the Add/Edit Failover Group dialog box to define failover groups for an Active/Active failover configuration.

**Fields**

- **Preferred Role**—Specifies the unit in the failover pair, primary or secondary, on which the failover group appears in the active state. You can have both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, balancing the traffic across the devices.
- **Preempt after booting with optional delay of**—Checking this check box causes the unit that is the preferred failover device for a failover group to become the active unit after rebooting. Checking this check box also enables the Preempt after booting with optional delay of field in which you can specify a period of time that the device should wait before becoming the active unit.
- **Preempt after booting with optional delay of**—Specifies the number of seconds that a unit should wait after rebooting before taking over as the active unit for any failover groups for which it is the preferred failover device. The range is between 0 and 1200 seconds.
- **Interface Policy**—Contains the fields for defining the policy for failover when monitoring detects an interface failure. These settings override any interface policy settings on the Criteria tab.
  - **Number of failed interfaces that triggers failover**—When the number of failed monitored interfaces exceeds the value you set with this command, then the security appliance fails over. The range is between 1 and 250 failures.
  - **Percentage of failed interfaces that triggers failover**—When the number of failed monitored interfaces exceeds the percentage you set with this command, then the security appliance fails over.
- **Poll time interval for monitored interfaces**—The amount of time between polls among interfaces. The range is between 1 and 15 seconds.
- **Enable HTTP replication**—Checking this check box enables Stateful Failover to copy active HTTP sessions to the standby firewall. If you do not allow HTTP replication, then HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link. This setting overrides the HTTP replication setting on the Setup tab.
- **MAC Addresses**—Lists physical interfaces on the security appliance for which an active and standby virtual MAC address has been configured.
  - **Physical Interface**—Displays the physical interface for which failover virtual MAC addresses are configured.

- Active MAC Address—Displays the MAC address for the interface and failover group on the unit where the failover group is active.
- Standby MAC Address—Displays the MAC address for the interface and failover group on the unit where the failover group is in the standby state.
- Add—Displays the Add Interface MAC Address dialog box. You cannot assign virtual MAC addresses to the LAN failover and Stateful Failover interfaces. See [Add/Edit Interface MAC Address](#) for more information.
- Edit—Displays the Edit Interface MAC Address dialog box for the selected interface. See [Add/Edit Interface MAC Address](#) for more information.
- Delete—Removes the currently selected interface from the MAC addresses table. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Add/Edit Interface MAC Address

Use the Add/Edit Interface MAC Address dialog box to define the active and standby virtual MAC addresses for the interfaces in a failover group. If you do not specify a virtual MAC address for an interface, the interface is given a default virtual MAC address as follows:

- Active unit default MAC address: 00a0.c9`physical_port_number.failover_group_id`01.
- Standby unit default MAC address: 00a0.c9:`physical_port_number.failover_group_id`02.



### Note

If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address.

These MAC addresses override the physical MAC addresses for the interface.

### Fields

- Physical Interface—Specifies the physical interface for which you are defining failover virtual MAC addresses. Because the MAC addresses do not change for the LAN failover and Stateful Failover interfaces during failover, you cannot choose these interfaces.
- MAC Addresses—Contains the fields for specifying the active and standby virtual MAC addresses for the interface.

- **Active Interface**—Specifies the MAC address for the interface and failover group on the unit where the failover group is active. Each interface may have up to two MAC addresses, one for each failover group, which override the physical MAC address. Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).
- **Standby Interface**—Specifies the MAC address for the interface and failover group on the unit where the failover group is in the standby state. Each interface may have up to two MAC addresses, one for each failover group, which override the physical MAC address. Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Failover > MAC Addresses Tab

The MAC Addresses tab lets you configure the virtual MAC addresses for the interfaces in an Active/Standby failover pair.

In Active/Standby failover, the MAC addresses for the primary unit are always associated with the active IP addresses. If the secondary unit boots first and becomes active, it uses the burned-in MAC address for its interfaces. When the primary unit comes online, the secondary unit obtains the MAC addresses from the primary unit. The change can disrupt network traffic.

You can configure virtual MAC addresses for each interface to ensure that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit. If you do not specify virtual MAC addresses, then the failover pair uses the burned-in NIC address as the MAC address.



### Note

You cannot configure a virtual MAC address for the failover or state links. The MAC and IP addresses for those links do not change during failover.

In Active/Active failover, the MAC addresses configured on this tab are not in effect. Instead, the MAC addresses defined in the failover groups are used.

### Fields

- **MAC Addresses**—Lists physical interfaces on the security appliance for which an active and standby virtual MAC address has been configured.
  - **Physical Interface**—Identifies the physical interface for which failover virtual MAC addresses are configured.
  - **Active MAC Address**—Identifies the MAC address on the active security appliance (usually primary).

- Standby MAC Address—Identifies the MAC address on the standby security appliance (usually secondary).
- Add—Displays the [Add/Edit Interface MAC Address](#) dialog box.
- Edit—Displays the [Add/Edit Interface MAC Address](#) dialog box for the selected interface.
- Delete—Removes the currently selected interface from the MAC addresses table. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

### For More Information

For more information about failover in general, see [Understanding Failover](#).

## Add/Edit Interface MAC Address

Use the Add/Edit Interface MAC Address dialog box to define the active and standby virtual MAC addresses for an interface.

### Fields

- Physical Interface—Specifies the physical interface for which you are defining failover virtual MAC addresses. Because the MAC addresses do not change for the LAN failover and Stateful Failover interfaces during failover, you cannot choose these interfaces.
- MAC Addresses—Contains the fields for specifying the active and standby virtual MAC addresses for the interface.
  - Active Interface—Specifies the MAC address of the interface on the active security appliance (usually primary). Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).
  - Standby Interface—Specifies the MAC address of the interface on the standby security appliance (usually secondary). Enter the MAC address in hexadecimal format (for example, 0123.4567.89AB).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | —                | —        | •      |

**For More Information**

For more information about failover in general, see [Understanding Failover](#).



# CHAPTER 16

## Configuring Management Access

---

This chapter contains the following topics:

- [Configuring Device Access, page 16-1](#)
- [Configuring CLI Parameters, page 16-2](#)
- [Configuring File Access, page 16-4](#)
- [Configuring ICMP Access, page 16-7](#)
- [Configuring a Management Interface, page 16-9](#)
- [Configuring SNMP, page 16-9](#)
- [Configuring Management Access Rules, page 16-19](#)
- [Configuring AAA for System Administrators, page 16-20](#)

## Configuring Device Access

To configure access to the security appliance, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH pane, click **Add**.
- The Add Device Access Configuration dialog box appears in the right-hand pane.
- Step 2** Choose the type of session from the three options listed: ASDM/HTTPS, Telnet, or SSH.
- Step 3** From the Interface Name drop-down list, choose the interface to use for administrative access.
- Step 4** In the IP Address field, add the IP address of the network or host that is allowed access.
- Step 5** From the Mask drop-down list, choose the mask associated with the network or host that is allowed access.
- Step 6** For ASDM/HTTPS sessions, verify that the Enable HTTP Server check box is checked (this is the default setting).
- Step 7** Make sure that port number 443 is specified (this is the default setting).
- Step 8** For Telnet sessions, the default timeout value is 5 minutes. To change this value, type a new one in the Telnet Timeout field.
- Step 9** For SSH sessions, choose the allowed SSH version(s) from the drop-down list.
- Step 10** For SSH sessions, the default timeout value is 60 minutes. To change this value, type a new one in the SSH Timeout field.

**Step 11** Click **Apply**.

The changes are saved to the running configuration.

---

## Configuring CLI Parameters

This section includes the following topics:

- [Adding a Banner, page 16-2](#)
- [Customizing a CLI Prompt, page 16-3](#)
- [Changing the Console Timeout Period, page 16-4](#)

## Adding a Banner

You can configure a message to display when a user connects to the security appliance, before a user logs in, or before a user enters privileged EXEC mode.

See the following guidelines:

- From a security perspective, it is important that your banner discourage unauthorized access. Do not use the words welcome or please, as they appear to invite intruders in. The following banner sets the correct tone for unauthorized access:  

```
You have logged in to a secure device. If you are not authorized to access this
device,
log out immediately or risk possible criminal consequences.
```
- See RFC 2196 for guidelines about banner messages.
- Only ASCII characters are allowed, including new line (Enter), which counts as two characters.
- Do not use tabs in the banner, because they are not preserved in the CLI version.
- There is no length limit for banners other than those for RAM and flash memory.
- You can dynamically add the hostname or domain name of the security appliance by including the strings \$(hostname) and \$(domain).
- If you configure a banner in the system configuration, you can use that banner text within a context by using the \$(system) string in the context configuration
- After a banner is added, security appliance Telnet or SSH sessions may close if:
  - There is not enough system memory available to process the banner message(s).
  - A TCP write error occurs when attempting to display banner message(s).

To add a message of the day, login, or session banner, perform the following steps:

---

**Step 1** From the Configuration > Device Management > Management Access > Command Line (CLI) > Banner pane, add your banner text to the field for the type of banner you are creating for the CLI:

- Session (exec) banner—This banner appears when a user accesses privileged EXEC mode at the CLI.
- Login Banner—This banner appears when a user logs in to the CLI.
- Message-of-the-day (motd) Banner—This banner appears when a user first connects to the CLI.



- **ASDM Banner**—This banner appears when a user connects to ASDM, following user authentication. The user is given two options for dismissing the banner:
  - **Continue**—Dismiss the banner and complete login as usual.
  - **Disconnect**—Dismiss the banner and terminate the connection.

**Step 2** Click **Apply**.

The banner is added and the changes are saved to the running configuration.

## Customizing a CLI Prompt

The CLI Prompt pane lets you customize the prompt used during CLI sessions. By default, the prompt shows the hostname of the security appliance. In multiple context mode, the prompt also displays the context name. You can display the following items in the CLI prompt.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>context</b>  | (Multiple mode only) Displays the name of the current context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>domain</b>   | Displays the domain name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>hostname</b> | Displays the hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>priority</b> | Displays the failover priority as pri (primary) or sec (secondary).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>state</b>    | Displays the traffic-passing state of the unit. The following values are displayed for the state: <ul style="list-style-type: none"> <li>• <b>act</b>—Failover is enabled, and the unit is actively passing traffic.</li> <li>• <b>stby</b>—Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state.</li> <li>• <b>actNoFailover</b>—Failover is not enabled, and the unit is actively passing traffic.</li> <li>• <b>stbyNoFailover</b>—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit.</li> </ul> |

To customize the prompt used during CLI sessions so that it shows something other than the hostname or context name, complete the following steps:

**Step 1** From the Configuration > Device Management > Management Access > CLI Prompt pane, do any of the following to customize the prompt:

- To add an attribute to the prompt, click the attribute in the Available Prompts list and then click **Add**. You can add multiple attributes to the prompt. The attribute is moved from the Available Prompts list to the Selected Prompts list.
- To remove an attribute from the prompt, click the attribute in the Selected Prompts list and then click **Delete**. The attribute is moved from the Selected Prompts list to the Available Prompts list.
- To change the order in which the attributes appear in the command prompt, click the attribute in the Selected Prompts list and click **Move Up** or **Move Down** to change the order.

The prompt is changed and displays in the CLI Prompt Preview field.

**Step 2** Click **Apply**.

The new prompt is saved to the running configuration.

---

## Changing the Console Timeout Period

To change the console timeout period, or the duration of time the management console remains active before automatically shutting down, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout pane, add a new timeout value in minutes.
- To specify unlimited, enter 0. The default value is 0.
- Step 2** Click **Apply**.
- The console timeout is changed, and the changes are saved to the running configuration.
- 

## Configuring File Access

This section includes the following topics.

- [Configuring the FTP Client Mode, page 16-4](#)
- [Configuring the Security Appliance as a Secure Copy Server, page 16-5](#)
- [Configuring the Security Appliance as a TFTP Client, page 16-5](#)
- [Adding Mount Points, page 16-6](#)

## Configuring the FTP Client Mode

The security appliance can use FTP to upload or download image files or configuration files to or from an FTP server. In passive FTP, the client initiates both the control connection and the data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

To configure the FTP client to be in passive mode, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > FTP Client pane, check **Specify FTP mode as passive**.
- Step 2** Click **Apply**.
- The FTP client configuration is changed and the change is saved to the running configuration.
-

## Configuring the Security Appliance as a Secure Copy Server

You can enable the secure copy server on the security appliance. Only clients that are allowed to access the security appliance using SSH can establish a secure copy connection.

This implementation of the secure copy server has the following limitations:

- The server can accept and terminate connections for secure copy, but cannot initiate them.
- The server does not have directory support. The lack of directory support limits remote client access to the security appliance internal files.
- The server does not support banners.
- The server does not support wildcards.
- The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

To configure the security appliance as a Secure Copy (SCP) server, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > **Secure Copy (SCP) Server** pane, check **Enable secure copy server**.
- Step 2** Click **Apply**.

The changes are saved to the running configuration. The security appliance can function as an SCP server for transferring files from/to the device.

---

## Configuring the Security Appliance as a TFTP Client

TFTP is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. You can configure the security appliance as a TFTP *client* so that it can transfer a copy of its running configuration file to a TFTP *server* using File > Save Running Configuration to TFTP Client or Tools > Command Line Interface. In this way, you can back up and propagate configuration files to multiple security appliances.

The security appliance supports only one TFTP client. The full path to the TFTP client is specified in Configuration > Device Management > Management Access > File Access > TFTP Client. Once configured here, you can use a colon (:) to specify the IP address in the CLI **configure net** and **copy** commands. However, any other authentication or configuration of intermediate devices necessary for communication from the security appliance to the TFTP client is done apart from this function.

To configure the security appliance as a TFTP client for saving configuration files to a TFTP server, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > TFTP Client pane, check **Enable**.
- Step 2** From the Interface Name drop-down list, choose the interface to use as a TFTP client.
- Step 3** In the IP Address field, add the IP address of the TFTP server where configuration files will be saved.
- Step 4** In the Path field, add the path to the TFTP server where configuration files will be saved.  
For example: /tftpboot/asa/config3
- Step 5** Click **Apply**.

The changes are saved to the running configuration. This TFTP server will be used to save the security appliance configuration files. For more information, see [Save Running Configuration to TFTP Server, page 3-4](#).

---

## Adding Mount Points

Common Internet File System (CIFS) and File Transfer Protocol (FTP) mount points

This section includes the following topics:

- [Adding a CIFS Mount Point, page 16-6](#)
- [Adding an FTP Mount Point, page 16-6](#)

### Adding a CIFS Mount Point

To define a CIFS mount point, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > CIFS Mount Point**.
- The Add CIFS Mount Point dialog box appears.
- Step 2** Check **Enable mount point**.
- This option attaches the CIFS file system on the security appliance to the UNIX file tree.
- Step 3** In the Mount Point Name field, add the name of an existing CIFS location.
- Step 4** In the Server Name or IP Address field, add the name or IP address of the server where the mount point is located.
- Step 5** In the Share Name field, add the name of the folder on the CIFS server.
- Step 6** In the NT Domain Name field, add the name of the NT Domain where the server resides.
- Step 7** In the User Name field, add the name of the user authorized for file system mounting on the server.
- Step 8** In the Password field, add the password for the user authorized for file system mounting on the server.
- Step 9** In the Confirm Password field, add the password again.
- Step 10** Click **OK**.
- The Add CIFS Mount Point dialog box closes.
- Step 11** Click **Apply**.
- The mount point is added to the security appliance and the change is saved to the running configuration.
- 

### Adding an FTP Mount Point



**Note**

For an FTP mount point, the FTP Server must have a UNIX directory listing style. Microsoft FTP servers have a default of MS-DOS directory listing style.

---

To define an FTP mount point, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > FTP Mount Point**.  
The Add FTP Mount Point dialog box appears.
- Step 2** Check the **Enable** check box.  
This option attaches the FTP file system on the security appliance to the UNIX file tree.
- Step 3** In the Mount Point Name field, add the name of an existing FTP location.
- Step 4** In the Server Name or IP Address field, add the name or IP address of the server where the mount point is located.
- Step 5** In the Mode field, click the radio button for the FTP mode (Active or Passive). When you choose Passive mode, the client initiates both the FTP control connection and data connection. The server responds with the number of its listening port for this connection.
- Step 6** In the Path to Mount field, add the directory path name to the FTP file server.
- Step 7** In the User Name field, add the name of the user authorized for file system mounting on the server.
- Step 8** In the Password field, add the password for the user authorized for file system mounting on the server.
- Step 9** In the Confirm Password field, add the password again.
- Step 10** Click **OK**.  
The dialog box closes.
- Step 11** Click **Apply**.  
The mount point is added to the security appliance and the change is saved to the running configuration.
- 

## Configuring Configuring ICMP Access

By default, you can send ICMP packets to any security appliance interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address. You can protect the security appliance from attacks by limiting the addresses of hosts and networks that are allowed to have ICMP access to the security appliance.



### Note

For allowing ICMP traffic *through* the security appliance, see the [“Configuring Access Rules” section on page 20-7](#).

It is recommended that permission is always granted for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If you configure ICMP rules, then the security appliance uses a first match to the ICMP traffic followed by an implicit deny all. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP rule is not configured; in that case, a **permit** statement is assumed.

To configure ICMP access rules, perform the following steps:

- Step 1** From the Configuration > Device Management > Management Access > ICMP pane, click **Add**.  
If you want to insert a rule in the ICMP table, click the rule that the new rule will precede, and click **Insert**.  
The Create ICMP Rule dialog box appears in the right-hand pane.
- Step 2** From the ICMP Type drop-down list, choose the type of ICMP message for this rule.  
[Table 16-1](#) lists the types of ICMP messages.

**Table 16-1 ICMP Type Literals**

| ICMP Type | Literal              |
|-----------|----------------------|
| 0         | echo-reply           |
| 3         | unreachable          |
| 4         | source-quench        |
| 5         | redirect             |
| 6         | alternate-address    |
| 8         | echo                 |
| 9         | router-advertisement |
| 10        | router-solicitation  |
| 11        | time-exceeded        |
| 12        | parameter-problem    |
| 13        | timestamp-request    |
| 14        | timestamp-reply      |
| 15        | information-request  |
| 16        | information-reply    |
| 17        | mask-request         |
| 18        | mask-reply           |
| 31        | conversion-error     |
| 32        | mobile-redirect      |

- Step 3** From the Interface selection list, choose the destination security appliance interface the rule is to be applied to.
- Step 4** In the IP Address field, do one of the following:
- Add a specific IP address for the host or network.
  - Click **Any Address** and go to [Step 7](#).
- Step 5** From the Mask drop-down list, choose the network mask.
- Step 6** Click **OK**.  
The dialog box closes.

- Step 7** (Optional) To set ICMP unreachable message limits, set the following options. Increasing the rate limit, along with enabling the “Decrement time to live for a connection” option on the Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings dialog box, is required to allow a traceroute through the security appliance that shows the security appliance as one of the hops.
- **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
  - **Burst Size**—Sets the burst rate, between 1 and 10. This keyword is not currently used by the system, so you can choose any value.
- Step 8** Click **Apply**.
- The ICMP rule is added to the end of the ICMP table and the change is saved to the running configuration.
- 

## Configuring a Management Interface

A high-security interface can be identified to manage the security appliance. When a management interface is assigned, ASDM can run on it with a fixed IP address over an IPSec VPN tunnel. This is possible if VPN is configured on the security appliance and the external interface is using a dynamically assigned IP address. The management interface is also used when accessing and managing the security appliance securely from home using the VPN client.

To configure a management interface, perform the following steps:

- Step 1** From the **Configuration > Device Management > Management Access > Management Interface** pane, choose the interface with the highest security (the inside interface) from the **Management Access Interface** drop-down list.
- Step 2** Click **Apply**.
- The management interface is assigned and the change is saved to the running configuration.
- 

## Configuring SNMP

This section describes how to configure SNMP, and includes the following topics:

- [Information About SNMP, page 16-9](#)
- [Configuring an SNMP Agent and Management Station, page 17-16](#)
- [Configuring SNMP Traps, page 17-19](#)

## Information About SNMP

The Simple Network Management Protocol (SNMP) enables the monitoring of network devices from a central location. The security appliance supports network monitoring using SNMP Versions 1 and 2c, as well as traps and SNMP read access, but does not support SNMP write access.

You can configure the security appliance to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the security appliance. Use CiscoWorks for Windows or any other SNMP V1, MIB-II-compliant browser to receive SNMP traps and browse a MIB.

The security appliance has an SNMP agent that notifies designated management stations if events occur that are pre-defined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, identifying itself to the management stations.

The security appliance SNMP agent also replies when a management station asks for information.

This section includes the following topics:

- [Information About SNMP Terminology, page 16-10](#)
- [Information About the Management Information Base and Traps, page 16-10](#)

## Information About SNMP Terminology

The following terms are commonly used when working with SNMP.

| Term                | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management stations | The PCs or workstations set up to monitor SNMP events and manage devices such as the security appliance.                                                                                                                                                                                                                                                                                                         |
| SNMP Agent          | The SNMP server running on the security appliance. The agent responds to requests for information and actions from the management station. The agent also controls access to the its management information base (MIB), the collection of objects that can be viewed or changed by the SNMP manager.                                                                                                             |
| OID                 | The system object identifier (OID) that identifies a device to its a management station and indicates to users the source of information monitored and displayed.                                                                                                                                                                                                                                                |
| MIB                 | Management Information Bases, or standardized data structures, for collecting information about packets, connections, buffers, failovers, etc. MIBs are defined by product and the protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs and request specific data or events be sent as they occur. Some MIB data can be modified for administrative purposes. |
| Trap                | Predefined events that generate a message from the SNMP agent to the management station. Events include alarm conditions such as link up, link down, or syslog event.                                                                                                                                                                                                                                            |
| Browsing            | Monitoring the health of a device from the management station by pulling required information from the device SNMP agent. This activity may include doing an snmpget or snmpwalk of the MIB tree from the management station.                                                                                                                                                                                    |

## Information About the Management Information Base and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. Standard traps are compiled into the security appliance software.

If needed, you can also download RFCs, standard MIBS, and standard traps from the IETF website: <http://www.ietf.org/>



Download Cisco MIBs from the following location:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Download Cisco OIDs from the following location:

<ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz>.

The following table describes the SNMP MIB support that the security appliance provides:

| MIB or Trap Support | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP core traps     | <p>The security appliance sends the following SNMP core traps:</p> <ul style="list-style-type: none"> <li>• authentication—An SNMP request fails because the NMS did not authenticate with the correct community string.</li> <li>• linkup—An interface has transitioned to the “up” state.</li> <li>• linkdown—An interface is down, for example, if you removed the <b>nameif</b> command.</li> <li>• coldstart—The adaptive security appliance is running after a reload.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| IF-MIB              | <p>Browsing of the following tables:</p> <ul style="list-style-type: none"> <li>• ifXTable</li> </ul> <p>The following objects are supported:</p> <pre> IF-MIB::ifName.1 = Ge7/0 IF-MIB::ifInMulticastPkts.1 = Counter32: 0 IF-MIB::ifInBroadcastPkts.1 = Counter32: 0 IF-MIB::ifOutMulticastPkts.1 = Counter32: 0 IF-MIB::ifOutBroadcastPkts.1 = Counter32: 0 IF-MIB::ifHCInOctets.1 = Counter64: 231678 IF-MIB::ifHCInUcastPkts.1 = Counter64: 963 IF-MIB::ifHCInMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCInBroadcastPkts.1 = Counter64: 0 IF-MIB::ifHCOctets.1 = Counter64: 27251 IF-MIB::ifHCOUcastPkts.1 = Counter64: 325 IF-MIB::ifHCOMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCOBroadcastPkts.1 = Counter64: 0 IF-MIB::ifLinkUpDownTrapEnable.1 = enabled(1) IF-MIB::ifHighSpeed.1 = Gauge32: 10000 (supports 10GE interfaces) IF-MIB::ifPromiscuousMode.1 = false(2) IF-MIB::ifConnectorPresent.1 = true(1) IF-MIB::ifAlias.1 = IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00 </pre> |

| MIB or Trap Support | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RFC1213-MIB         | <p>Browsing of the following table:</p> <ul style="list-style-type: none"> <li>ip.ipAddrTable</li> <li>ifTable</li> </ul> <p>The following objects are supported:</p> <pre> RFC1213-MIB::ifNumber.0 = 1 RFC1213-MIB::ifIndex.1 = 1 RFC1213-MIB::ifDescr.1 = "Adaptive Security Appliance 'mgmt' interface" RFC1213-MIB::ifType.1 = ethernet-csmacd(6) RFC1213-MIB::ifMtu.1 = 1500 RFC1213-MIB::ifSpeed.1 = Gauge32: 4294967295 RFC1213-MIB::ifPhysAddress.1 = Hex: 00 15 17 15 AB 08 RFC1213-MIB::ifAdminStatus.1 = up(1) RFC1213-MIB::ifOperStatus.1 = up(1) RFC1213-MIB::ifLastChange.1 = Timeticks: (200) 0:00:02.00 RFC1213-MIB::ifInOctets.1 = Counter32: 231678 RFC1213-MIB::ifInUcastPkts.1 = Counter32: 963 RFC1213-MIB::ifInNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifInDiscards.1 = Counter32: 630 RFC1213-MIB::ifInErrors.1 = Counter32: 0 RFC1213-MIB::ifOutOctets.1 = Counter32: 27251 RFC1213-MIB::ifOutUcastPkts.1 = Counter32: 325 RFC1213-MIB::ifOutNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifOutDiscards.1 = Counter32: 0 RFC1213-MIB::ifOutErrors.1 = Counter32: 0 RFC1213-MIB::ifOutQLen.1 = Gauge32: 6 RFC1213-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero </pre> <ul style="list-style-type: none"> <li>system</li> </ul> <p>The following objects are supported:</p> <pre> RFC1213-MIB::sysDescr.0 = "Cisco Adaptive Security Appliance Version 8.1(0)15" RFC1213-MIB::sysObjectID.0 = OID: CISCO-PRODUCTS-MIB::ciscoASA5580 RFC1213-MIB::sysUpTime.0 = Timeticks: (390500) 1:05:05.00 RFC1213-MIB::sysContact.0 = "yourname@yourcompany.com" RFC1213-MIB::sysName.0 = "sw8-5580" RFC1213-MIB::sysLocation.0 = "YourCity, YourState" RFC1213-MIB::sysServices.0 = 4 </pre> |
| SNMPv2-MIB          | SNMP browsing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| MIB or Trap Support | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENTITY-MIB          | <p>Browsing of the following groups and tables:</p> <ul style="list-style-type: none"> <li>entPhysicalTable</li> <li>entLogicalTable</li> </ul> <p>The following objects are supported:</p> <pre> ENTITY-MIB::entPhysicalDescr.1 = ASA 5580 Series SPE40 or SPE20 ENTITY-MIB::entPhysicalDescr.2 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.3 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.4 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.5 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.6 = ASA 5580 4 port GE Fiber If Card ENTITY-MIB::entPhysicalDescr.7 = ASA 5580 4 port GE Copper If Card ENTITY-MIB::entPhysicalDescr.8 = ASA 5580 2 port 10GE SR Fiber If Card ENTITY-MIB::entPhysicalVendorType.1 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevChassisASA5580 ENTITY-MIB::entPhysicalVendorType.2 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.3 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.4 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.5 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.6 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm4xlgeFi ENTITY-MIB::entPhysicalVendorType.7 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm4xlgeCu ENTITY-MIB::entPhysicalVendorType.8 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm2x10geFi ENTITY-MIB::entPhysicalContainedIn.1 = 0 ENTITY-MIB::entPhysicalContainedIn.2 = 1 ENTITY-MIB::entPhysicalContainedIn.3 = 1 ENTITY-MIB::entPhysicalContainedIn.4 = 1 ENTITY-MIB::entPhysicalContainedIn.5 = 1 ENTITY-MIB::entPhysicalContainedIn.6 = 1 ENTITY-MIB::entPhysicalContainedIn.7 = 1 ENTITY-MIB::entPhysicalContainedIn.8 = 1 ENTITY-MIB::entPhysicalClass.1 = chassis(3) ENTITY-MIB::entPhysicalClass.2 = cpu(12) ENTITY-MIB::entPhysicalClass.3 = cpu(12) ENTITY-MIB::entPhysicalClass.4 = cpu(12) ENTITY-MIB::entPhysicalClass.5 = cpu(12) ENTITY-MIB::entPhysicalClass.6 = module(9) ENTITY-MIB::entPhysicalClass.7 = module(9) ENTITY-MIB::entPhysicalClass.8 = module(9) ENTITY-MIB::entPhysicalParentRelPos.1 = 0 ENTITY-MIB::entPhysicalParentRelPos.2 = 0 ENTITY-MIB::entPhysicalParentRelPos.3 = 1 ENTITY-MIB::entPhysicalParentRelPos.4 = 2 ENTITY-MIB::entPhysicalParentRelPos.5 = 3 ENTITY-MIB::entPhysicalParentRelPos.6 = 0 ENTITY-MIB::entPhysicalParentRelPos.7 = 0 ENTITY-MIB::entPhysicalParentRelPos.8 = 0 ENTITY-MIB::entPhysicalName.1 = Chassis ENTITY-MIB::entPhysicalName.2 = 0 ENTITY-MIB::entPhysicalName.3 = 1 ENTITY-MIB::entPhysicalName.4 = 2 </pre> |

| MIB or Trap Support    | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENTITY-MIB (continued) | <p> ENTITY-MIB::entPhysicalName.5 = 3<br/> ENTITY-MIB::entPhysicalName.6 = slot 4<br/> ENTITY-MIB::entPhysicalName.7 = slot 5<br/> ENTITY-MIB::entPhysicalName.8 = slot 7<br/> ENTITY-MIB::entPhysicalHardwareRev.1 = V01<br/> ENTITY-MIB::entPhysicalHardwareRev.2 =<br/> ENTITY-MIB::entPhysicalHardwareRev.3 =<br/> ENTITY-MIB::entPhysicalHardwareRev.4 =<br/> ENTITY-MIB::entPhysicalHardwareRev.5 =<br/> ENTITY-MIB::entPhysicalHardwareRev.6 = D5618404<br/> ENTITY-MIB::entPhysicalHardwareRev.7 = D4577407<br/> ENTITY-MIB::entPhysicalHardwareRev.8 = D7555203<br/> ENTITY-MIB::entPhysicalFirmwareRev.1 = 1.1(0)4<br/> ENTITY-MIB::entPhysicalFirmwareRev.2 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.3 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.4 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.5 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.6 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.7 =<br/> ENTITY-MIB::entPhysicalFirmwareRev.8 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.1 = 8.1(0)1<br/> ENTITY-MIB::entPhysicalSoftwareRev.2 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.3 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.4 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.5 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.6 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.7 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.8 =<br/> ENTITY-MIB::entPhysicalSerialNum.1 = JAB12345678<br/> ENTITY-MIB::entPhysicalSerialNum.2 =<br/> ENTITY-MIB::entPhysicalSerialNum.3 =<br/> ENTITY-MIB::entPhysicalSerialNum.4 =<br/> ENTITY-MIB::entPhysicalSoftwareRev.5 =<br/> ENTITY-MIB::entPhysicalSerialNum.6 = 001517154451<br/> ENTITY-MIB::entPhysicalSerialNum.7 = 0015171559DC<br/> ENTITY-MIB::entPhysicalSerialNum.8 = 0015171D9752<br/> ENTITY-MIB::entPhysicalMfgName.1 = Cisco Systems Inc.<br/> ENTITY-MIB::entPhysicalMfgName.2 =<br/> ENTITY-MIB::entPhysicalMfgName.3 =<br/> ENTITY-MIB::entPhysicalMfgName.4 =<br/> ENTITY-MIB::entPhysicalMfgName.5 =<br/> ENTITY-MIB::entPhysicalMfgName.6 =<br/> ENTITY-MIB::entPhysicalMfgName.7 =<br/> ENTITY-MIB::entPhysicalMfgName.8 =<br/> ENTITY-MIB::entPhysicalMfgName.9 =<br/> ENTITY-MIB::entPhysicalModelName.1 = ASA5580-SPE40 or SPE20<br/> ENTITY-MIB::entPhysicalModelName.2 =<br/> ENTITY-MIB::entPhysicalModelName.3 =<br/> ENTITY-MIB::entPhysicalModelName.4 =<br/> ENTITY-MIB::entPhysicalModelName.5 =<br/> ENTITY-MIB::entPhysicalModelName.6 = ASA5580-4GE-FI<br/> ENTITY-MIB::entPhysicalModelName.7 = ASA5580-4GE-CU<br/> ENTITY-MIB::entPhysicalModelName.8 = ASA5580-2X10GE-SR<br/> ENTITY-MIB::entPhysicalAlias.1 =<br/> ENTITY-MIB::entPhysicalAlias.2 =<br/> ENTITY-MIB::entPhysicalAlias.3 =<br/> ENTITY-MIB::entPhysicalAlias.4 =<br/> ENTITY-MIB::entPhysicalAlias.5 =<br/> ENTITY-MIB::entPhysicalAlias.6 =<br/> ENTITY-MIB::entPhysicalAlias.7 = </p> |

| MIB or Trap Support             | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENTITY-MIB (continued)          | <p>ENTITY-MIB::entPhysicalAlias.8 =<br/> ENTITY-MIB::entPhysicalAssetID.1 =<br/> ENTITY-MIB::entPhysicalAssetID.2 =<br/> ENTITY-MIB::entPhysicalAssetID.3 =<br/> ENTITY-MIB::entPhysicalAssetID.8 =<br/> ENTITY-MIB::entPhysicalIsFRU.1 = false(2)<br/> ENTITY-MIB::entPhysicalIsFRU.2 = false(2)<br/> ENTITY-MIB::entPhysicalIsFRU.4 = false(2)<br/> ENTITY-MIB::entPhysicalIsFRU.5 = false(2)<br/> ENTITY-MIB::entPhysicalIsFRU.6 = true(1)<br/> ENTITY-MIB::entPhysicalIsFRU.7 = true(1)<br/> ENTITY-MIB::entPhysicalIsFRU.8 = true(1)</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• config-change</li> <li>• fru-insert</li> <li>• fru-remove</li> </ul> |
| CISCO-IPSEC-FLOW-MONITOR-MIB    | <p>Browsing of the MIB.</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• start</li> <li>• stop</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CISCO-REMOTE-ACCESS-MONITOR-MIB | <p>Browsing of the MIB.</p> <p>Browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• session-threshold-exceeded</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CISCO-CRYPTO-ACCELERATOR-MIB    | Browsing of the MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ALTIGA-GLOBAL-REG               | Browsing of the MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CISCO-FIREWALL-MIB              | <p>Browsing of the following groups:</p> <ul style="list-style-type: none"> <li>• cfwSystem</li> </ul> <p>The information in cfwSystem.cfwStatus, which relates to failover status, applies to the entire device and not just a single context.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| MIB or Trap Support   | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-MEMORY-POOL-MIB | <p>Browsing of the following table:</p> <ul style="list-style-type: none"> <li>ciscoMemoryPoolTable—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors.</li> </ul> <p>The following objects are supported:</p> <pre> CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.1 = System memory CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.6 = DMA ALT1 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.7 = DMA CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.8 = Global Shared CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.1 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.6 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.7 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.8 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.1 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.6 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.7 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.8 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.1 = Gauge32: 102805792 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.6 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.7 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.8 = Gauge32: 38752248 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.1 = Gauge32: 1432686304 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.6 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.7 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.8 = Gauge32: 229683208 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.1 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.6 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.7 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.8 = Gauge32: 0 bytes </pre> |

| MIB or Trap Support        | Description of Security Appliance Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-PROCESS- MIB         | <p>Browsing of the following table:</p> <ul style="list-style-type: none"> <li>cpmCPUTotalTable</li> </ul> <p>The following objects are supported:</p> <pre> CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.1 = 1 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.2 = 2 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.3 = 3 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.4 = 4 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.5 = 5 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.6 = 1 CISCO-PROCESS-MIB::cpmCPUTotal5sec.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal5sec.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal5sec.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal1min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal1min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal5min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal5min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.6 = Gauge32: 50 </pre> <p>The first row in the cpmCPUTotalTable reflects either the CPU load for the system in single security context mode or the CPU load for the context in multiple context mode.</p> <p>The last row in cpmCPUTotalTable always reflects the system CPU load. This row is identical to the first row in single context mode and is only available through the admin context in multiple context mode. The row represents the load for all CPUs, and is equivalent to the output from the <b>show cpu</b> command.</p> <p>All rows in-between the first and last reflect the per-CPU load. They are only present for multi-CPU systems and only available in either single mode or the admin context in multiple mode.</p> |
| CISCO-SYSLOG-MIB           | <p>The following trap:</p> <ul style="list-style-type: none"> <li>clogMessageGenerated</li> </ul> <p>You cannot browse this MIB.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CISCO-UNIFIED-FIREWALL-MIB | <p>Browsing of the following tables:</p> <ul style="list-style-type: none"> <li>cuFwConnectionGlobals</li> <li>cufwUrlFilterGlobals</li> <li>cufwUrlFilterServers</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring an SNMP Agent and Management Station

This section includes the following topics:

- [Configuring the SNMP Agent, page 16-18](#)

- [Adding an SNMP Management Station, page 16-18](#)

## Configuring the SNMP Agent

To configure an SNMP agent, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, in the Community String (default) field, add a default community string.
- Enter the password used by the SNMP management stations when sending requests to the security appliance. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security appliance uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default is "public." SNMPv2c allows separate community strings to be set for each management station. If no community string is configured for any management station, the value set here will be used by default.
- Step 2** In the Contact field, add the name of the security appliance system administrator. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- Step 3** In the Location field, add the location of the security appliance being managed by SNMP. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- Step 4** In the Listening Port field, add the number of the security appliance port that listens for SNMP requests from management stations; or keep the default, port number 161.
- Step 5** Click **Apply**.
- The SNMP agent is configured and the changes are saved to the running configuration.
- 

## Adding an SNMP Management Station

To add an SNMP management station, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, Click **Add**. The Add SNMP Host Access Entry dialog box appears.
- Step 2** From the Interface Name drop-down menu, choose the interface where the SNMP host resides.
- Step 3** In the IP Address field, add the SNMP host IP address.
- Step 4** In the UDP Port field, add the SNMP host UDP port, or keep the default, port 162.
- Step 5** In the Community String field, add the SNMP host community string. If no community string is specified for a management station, the value set in Community String (default) field on the SNMP pane will be used.
- Step 6** From the SNMP Version drop-down menu, choose the SNMP version used by the SNMP host.
- Step 7** Check the Poll or Trap check boxes to specify the method for communicating with this management station.
- Step 8** Click **OK**.
- The dialog box closes.



- Step 9** Click **Apply**.  
The management station is configured and changes are saved to the running configuration.
- 

## Configuring SNMP Traps

To designate which traps the SNMP agent generates and how they are collected and sent to network management stations, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > SNMP pane, click **Configure Traps**.  
The SNMP Trap Configuration dialog box appears.
- Step 2** Click the SNMP events to notify through SNMP traps.
- Step 3** Click **OK**.  
The dialog box closes.
- Step 4** Click **Apply**.  
The SNMP traps are configured and the changes are saved to the running configuration.
- 

## Configuring Management Access Rules

Access Rules specifically permit or deny traffic to or from a particular peer (or peers) while Management Access Rules provide access control for to-the-box traffic. For example, in addition to detecting IKE Denial of Service attacks, you can block them using management access rules.

To add a Management Access Rule, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > Management Access Rules pane, from the Add menu, click **Add Management Access Rule**.  
The Add Management Access Rules dialog box appears.
- Step 2** From the Interface drop-down list, choose an interface for applying the rule.
- Step 3** In the Action field, click one of the following:
- **Permit** (permits this traffic)
  - **Deny** (denies this traffic)
- Step 4** In the Source field, choose Any, or click the ellipsis (...) to browse for an address.
- Step 5** In the Service field, add a service name for the rule traffic, or click the ellipsis (...) to browse for a service.
- Step 6** (Optional) In the Description field, add a description for this management access rule.
- Step 7** (Optional) If you want to receive log messages for this management access rule, check **Enable Logging** and then from the Logging Level drop-down list, choose the level of logging to apply to this rule.

- Step 8** (Optional) To configure advanced options, click **More Options**. You can configure the following settings:
- If you want to turn off this Management Access Rule, uncheck **Enable Rule**.
  - To add a source service in the Source Service field; or click the ellipsis (...) to browse for a source service.  
The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
  - To configure the logging interval (if you enable logging and choose a non-default setting), enter a value in seconds in the Logging Interval field.
  - To select a predefined time range for this rule, from the Time Range drop-down list, choose a time range; or click the ellipsis (...) to browse for a time range.  
The Add Time Range dialog box appears. For information about adding a time range, see [Configuring Time Ranges, page 19-15](#).
- Step 9** Click **OK**.  
The dialog box closes and the Management Access rule is added.
- Step 10** Click **Apply**.  
The rule is saved in the running configuration.
- 

## Configuring AAA for System Administrators

This section describes how to enable authentication and command authorization for system administrators. Before you configure AAA for system administrators, first configure the local database or AAA server according to the [“Configuring the Local Database” section on page 12-7](#) or the [“Identifying AAA Server Groups and Servers” section on page 12-12](#).

This section includes the following topics:

- [Configuring Authentication for CLI, ASDM, and enable command Access, page 16-20](#)
- [Limiting User CLI and ASDM Access with Management Authorization, page 16-22](#)
- [Configuring Command Authorization, page 16-23](#)
- [Configuring Management Access Accounting, page 16-31](#)
- [Recovering from a Lockout, page 16-32](#)

## Configuring Authentication for CLI, ASDM, and enable command Access

If you enable CLI authentication, the security appliance prompts you for your username and password to log in. After you enter your information, you have access to user EXEC mode.

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

If you configure **enable** authentication, the security appliance prompts you for your username and password. If you do not configure **enable** authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use **enable** authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use **enable** authentication.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.

**Note**

Before the security appliance can authenticate a Telnet, SSH, or HTTP user, you must first configure access to the security appliance according to the “[Configuring Device Access](#)” section on page 16-1. These panes identify the IP addresses that are allowed to communicate with the security appliance.

To configure CLI, ASDM, or **enable** authentication, perform the following steps:

- 
- Step 1** To authenticate users who use the **enable** command, go to Configuration > Device Management > Users/AAA > AAA Access > Authentication, and configure the following settings:
- a. Check the **Enable** check box.
  - b. From the Server Group drop-down list, choose a server group name or the LOCAL database.
  - c. (Optional) If you chose a AAA server, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used.
- Step 2** To authenticate users who access the CLI or ASDM, go to Configuration > Device Management > Users/AAA > AAA Access > Authentication, and configure the following settings:
- a. Check one or more of the following check boxes:
    - **HTTP/ASDM**—Authenticates the ASDM client that accesses the security appliance using HTTPS. You only need to configure HTTP authentication if you want to use a AAA server. By default, ASDM uses the local database for authentication even if you do not configure this command. HTTP management authentication does not support the SDI protocol for a AAA server group.
    - **Serial**—Authenticates users who access the security appliance using the console port.
    - **SSH**—Authenticates users who access the security appliance using SSH.
    - **Telnet**—Authenticates users who access the security appliance using Telnet.
  - b. For each service that you checked, from the Server Group drop-down list, choose a server group name or the LOCAL database.
  - c. (Optional) If you chose a AAA server, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used.
- Step 3** Click **Apply**.
-

## Limiting User CLI and ASDM Access with Management Authorization

If you configure CLI or **enable** authentication, you can limit a local user, RADIUS, TACACS+, or LDAP user (if you map LDAP attributes to RADIUS attributes) from accessing the CLI, ASDM, or the **enable** command.

**Note**

Serial access is not included in management authorization, so if you enable the Authentication > Serial option, then any user who authenticates can access the console port.

To configure management authorization, perform the following steps:

- Step 1** To enable management authorization, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check the **Perform authorization for exec shell access > Enable** check box.

This option also enables support of administrative user privilege levels from RADIUS, which can be used in conjunction with local command privilege levels for command authorization. See the [“Configuring Local Command Authorization” section on page 16-25](#) for more information.

- Step 2** To configure the user for management authorization, see the following requirements for each AAA server type or local user:
- RADIUS or LDAP (mapped) users—Configure the Service-Type attribute for one of the following values.
    - admin—Allows full access to any services specified by the Authentication tab options.
    - nas-prompt—Allows access to the CLI when you configure the Telnet or SSH authentication options, but denies ASDM configuration access if you configure the HTTP option. ASDM monitoring access is allowed. If you configure **enable** authentication with the Enable option, the user cannot access privileged EXEC mode using the **enable** command.
    - remote-access—Denies management access. The user cannot use any services specified by the Authentication tab options (excluding the Serial option; serial access is allowed).
  - TACACS+ users—Authorization is requested with the “service=shell” and the server responds with PASS or FAIL.
    - PASS, privilege level 1—Allows full access to any services specified by the Authentication tab options.
    - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the Telnet or SSH authentication options, but denies ASDM configuration access if you configure the HTTP option. ASDM monitoring access is allowed. If you configure **enable** authentication with the Enable option, the user cannot access privileged EXEC mode using the **enable** command.
    - FAIL—Denies management access. The user cannot use any services specified by the Authentication tab options (excluding the Serial option; serial access is allowed).
  - Local users—Configure the Access Restriction option. See the [“Add/Edit User Account > Identity” section on page 12-9](#). By default, the access restriction is Full Access, which allows full access to any services specified by the Authentication tab options.

## Configuring Command Authorization

If you want to control the access to commands, the security appliance lets you configure command authorization, where you can determine which commands that are available to a user. By default when you log in, you can access user EXEC mode, which offers only minimal commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands.

This section includes the following topics:

- [Command Authorization Overview, page 16-23](#)
- [Configuring Local Command Authorization, page 16-25](#)
- [Configuring TACACS+ Command Authorization, page 16-27](#)

### Command Authorization Overview

This section describes command authorization, and includes the following topics:

- [Supported Command Authorization Methods, page 16-23](#)
- [About Preserving User Credentials, page 16-23](#)
- [Security Contexts and Command Authorization, page 16-24](#)

### Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the security appliance. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the security appliance places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user's privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the **enable** command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the **login** command (local database only).

**Note**

You can use local command authorization without any users in the local database and without CLI or **enable** authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the security appliance places you in level 15. You can then create enable passwords for every level, so that when you enter **enable n** (2 to 15), the security appliance places you in level *n*. These levels are not used unless you turn on local command authorization (see “[Configuring Local Command Authorization](#)” below). (See the *Cisco Security Appliance Command Reference* for more information about **enable**.)

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

### About Preserving User Credentials

When a user logs into the security appliance, they are required to provide a username and password for authentication. The security appliance retains these session credentials in case further authentication is needed later in the session.

When the following configurations are in place, a user needs only to authenticate with the local server upon login. Subsequent serial authorization uses the saved credentials. The user is also prompted for the privilege level 15 password. When exiting privileged mode, the user is authenticated again. User credentials are not retained in privileged mode.

- Local server is configured to authenticate user access.
- Privilege level 15 command access is configured to require a password.
- User's account is configured for serial only authorization (no access to console or ASDM).
- User's account is configured for privilege level 15 command access.

The following table shows how credentials are used in this case by the security appliance.

| Credentials required     | Username and Password Authentication | Serial Authorization | Privileged Mode Command Authorization | Privileged Mode Exit Authorization |
|--------------------------|--------------------------------------|----------------------|---------------------------------------|------------------------------------|
| Username                 | Yes                                  | No                   | No                                    | Yes                                |
| Password                 | Yes                                  | No                   | No                                    | Yes                                |
| Privileged Mode Password | No                                   | No                   | Yes                                   | No                                 |

## Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default "enable\_15" username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable\_15 user or if authorizations are different for the enable\_15 user than for the user in the previous context session.

This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable\_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable\_15 username. If you use different accounting servers for each context, tracking who was using the enable\_15 username requires correlating the data from several servers.

When configuring command authorization, consider the following:

- An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable\_15 user in each of the other contexts.

- If you intend to authorize commands differently per context, ensure that in each context the `enable_15` username is denied use of commands that are also denied to administrators who are permitted use of the **changeto** command.

When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.

**Note**

The system execution space does not support AAA commands; therefore, command authorization is not available in the system execution space.

## Configuring Local Command Authorization

Local command authorization lets you assign commands to one of 16 privilege levels (0 to 15). By default, each command is assigned either to privilege level 0 or 15. You can define each user to be at a specific privilege level, and each user can enter any command at their privilege level or below. The security appliance supports user privilege levels defined in the local database, a RADIUS server, or an LDAP server (if you map LDAP attributes to RADIUS attributes. See the [“Configuring an LDAP Attribute Map”](#) section on page 12-22.)

This section includes the following topics:

- [Local Command Authorization Prerequisites, page 16-25](#)
- [Default Command Privilege Levels, page 16-26](#)
- [Assigning Privilege Levels to Commands and Enabling Authorization, page 16-26](#)

### Local Command Authorization Prerequisites

Complete the following tasks as part of your command authorization configuration:

- Configure **enable** authentication. (See the [“Configuring Authentication for CLI, ASDM, and enable command Access”](#) section on page 16-20.)

**enable** authentication is essential to maintain the username after the user accesses the **enable** command.

Alternatively, you can use the **login** command (which is the same as the **enable** command with authentication; for the local database only), which requires no configuration. We do not recommend this option because it is not as secure as **enable** authentication.

You can also use CLI authentication, but it is not required.

- See the following prerequisites for each user type:
  - Local database users—Configure each user in the local database at a privilege level from 0 to 15. To configure the local database, see the [“Configuring the Local Database”](#) section on page 12-7.
  - RADIUS users—Configure the user with Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15.
  - LDAP users—Configure the user with a privilege level between 0 and 15, and then map the LDAP attribute to Cisco VAS CVPN3000-Privilege-Level according to the [“Configuring an LDAP Attribute Map”](#) section on page 12-22.

## Default Command Privilege Levels

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

## Assigning Privilege Levels to Commands and Enabling Authorization

To assign a command to a new privilege level, and enable authorization, follow these steps:

- 
- Step 1** To enable command authorization, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check **Enable authorization for command access > Enable**.
- Step 2** From the Server Group drop-down list, choose **LOCAL**.
- Step 3** When you enable local command authorization, you have the option of manually assigning privilege levels to individual commands or groups of commands or enabling the predefined user account privileges.
- To use predefined user account privileges, click **Set ASDM Defined User Roles**.  
The ASDM Defined User Roles Setup dialog box shows the commands and their levels. Click **Yes** to use the predefined user account privileges: Admin (privilege level 15, with full access to all CLI commands; Read Only (privilege level 5, with read-only access); and Monitor Only (privilege level 3, with access to the Monitoring section only).
  - To manually configure command levels, click **Configure Command Privileges**.  
The Command Privileges Setup dialog box appears. You can view all commands by choosing **--All Modes--** from the Command Mode drop-down list, or you can choose a configuration mode to view the commands available in that mode. For example, if you choose **context**, you can view all commands available in context configuration mode. If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately.



The Variant column displays show, clear, or cmd. You can set the privilege only for the show, clear, or configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form.

To change the level of a command, double-click it or click **Edit**. You can set the level between 0 and 15. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately.

To change the level of all shown commands, click **Select All** and then **Edit**.

Click **OK** to accept your changes.

- Step 4** To support administrative user privilege levels from RADIUS, check **Perform authorization for exec shell access > Enable**.

Without this option, the security appliance only supports privilege levels for local database users and defaults all other types of users to level 15.

This option also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users. See the [“Limiting User CLI and ASDM Access with Management Authorization” section on page 16-22](#) for more information.

- Step 5** Click **Apply**.
- 

## Configuring TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the security appliance sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the security appliance. If you still get locked out, see the [“Recovering from a Lockout” section on page 16-32](#).

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the security appliance. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels according to the [“Configuring Command Authorization” section on page 16-23](#).

This section includes the following topics:

- [TACACS+ Command Authorization Prerequisites, page 16-27](#)
- [Configuring Commands on the TACACS+ Server, page 16-28](#)
- [Enabling TACACS+ Command Authorization, page 16-30](#)

### TACACS+ Command Authorization Prerequisites

Configure CLI and **enable** authentication (see the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 16-20](#)).

## Configuring Commands on the TACACS+ Server

You can configure commands on a Cisco Secure Access Control Server (ACS) TACACS+ server as a shared profile component, for a group, or for individual users. For third-party TACACS+ servers, see your server documentation for more information about command authorization support.

See the following guidelines for configuring commands in Cisco Secure ACS Version 3.1; many of these guidelines also apply to third-party servers:

- The security appliance sends the commands to be authorized as “shell” commands, so configure the commands on the TACACS+ server as shell commands.



**Note** Cisco Secure ACS might include a command type called “pix-shell.” Do not use this type for security appliance command authorization.

- The first word of the command is considered to be the main command. All additional words are considered to be arguments, which need to be preceded by **permit** or **deny**.

For example, to allow the **show running-configuration aaa-server** command, add **show running-configuration** to the command box, and type **permit aaa-server** in the arguments box.

- You can permit all arguments of a command that you do not explicitly deny by selecting the **Permit Unmatched Args** check box.

For example, you can configure just the **show** command, and then all the **show** commands are allowed. We recommend using this method so that you do not have to anticipate every variant of a command, including abbreviations and **?**, which shows CLI usage (see [Figure 16-1](#)).

**Figure 16-1** Permitting All Related Commands

- For commands that are a single word, you *must* permit unmatched arguments, even if there are no arguments for the command, for example **enable** or **help** (see [Figure 16-2](#)).

**Figure 16-2**      **Permitting Single Word Commands**

The screenshot shows the Cisco ASDM configuration window for command permissions. On the left, under the 'Commands' tab, the word 'enable' is entered in the text box. On the right, under the 'Arguments' tab, the text box is empty. The 'Permit Unmatched Args' checkbox is checked. At the bottom, there are two buttons: 'Add Command' and 'Remove Command'. A small vertical label '114411' is on the right side of the window.

- To disallow some arguments, enter the arguments preceded by **deny**.

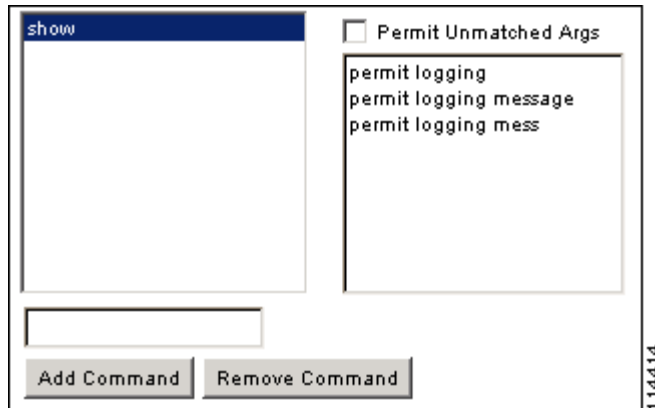
For example, to allow **enable**, but not **enable password**, enter **enable** in the commands box, and **deny password** in the arguments box. Be sure to select the Permit Unmatched Args check box so that **enable** alone is still allowed (see [Figure 16-3](#)).

**Figure 16-3**      **Disallowing Arguments**

The screenshot shows the Cisco ASDM configuration window for command permissions. On the left, under the 'Commands' tab, the word 'enable' is entered in the text box. On the right, under the 'Arguments' tab, the text 'deny password' is entered in the text box. The 'Permit Unmatched Args' checkbox is checked. At the bottom, there are two buttons: 'Add Command' and 'Remove Command'. A small vertical label '114410' is on the right side of the window.

- When you abbreviate a command at the command line, the security appliance expands the prefix and main command to the full text, but it sends additional arguments to the TACACS+ server as you enter them.

For example, if you enter **sh log**, then the security appliance sends the entire command to the TACACS+ server, **show logging**. However, if you enter **sh log mess**, then the security appliance sends **show logging mess** to the TACACS+ server, and not the expanded command **show logging message**. You can configure multiple spellings of the same argument to anticipate abbreviations (see [Figure 16-4](#)).

**Figure 16-4 Specifying Abbreviations**

- We recommend that you allow the following basic commands for all users:
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

### Enabling TACACS+ Command Authorization

Before you enable TACACS+ command authorization, be sure that you are logged into the security appliance as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the security appliance. For example, you should log in as an admin user with all commands authorized. Otherwise, you could become unintentionally locked out.

To configure TACACS+ command authorization, perform the following steps:

- 
- Step 1** To perform command authorization using a TACACS+ server, go to Configuration > Device Management > Users/AAA > AAA Access > Authorization, and check the **Enable authorization for command access > Enable** check box.
  - Step 2** From the Server Group drop-down list, choose a AAA server group name.
  - Step 3** (Optional) you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Click the **Use LOCAL when server group fails** check box. We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used.

**Step 4** Click **Apply**.

---

## Configuring Management Access Accounting

To enable accounting for management access, perform the following steps:

- 
- Step 1** You can only account for users that first authenticate with the security appliance, so configure authentication using the [“Configuring Authentication for CLI, ASDM, and enable command Access” section on page 16-20](#).
- Step 2** To enable accounting of users when they enter the **enable** command:
- Go to Configuration > Device Management > Users/AAA > AAA Access > Accounting, and check the **Require accounting to allow accounting of user activity > Enable** check box.
  - From the Server Group drop-down list, choose a RADIUS or TACACS+ server group name.
- Step 3** To enable accounting of users when they access the security appliance using Telnet, SSH, or the serial console:
- Under the Require accounting for the following types of connections area, check the check boxes for Serial, SSH, and/or Telnet.
  - For each connection type, from the Server Group drop-down list, choose a RADIUS or TACACS+ server group name.
- Step 4** To configure command accounting:
- Under the Require command accounting area, check **Enable**.
  - From the Server Group drop-down list, choose a TACACS+ server group name. RADIUS is not supported.  
  
You can send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI.
  - If you customize the command privilege level using the Command Privilege Setup dialog box (see the [“Assigning Privilege Levels to Commands and Enabling Authorization” section on page 16-26](#)), you can limit which commands the security appliance accounts for by specifying a minimum privilege level in the Privilege level drop-down list. The security appliance does not account for commands that are below the minimum privilege level.
- Step 5** Click **Apply**.
-

## Recovering from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the security appliance CLI. You can usually recover access by restarting the security appliance. However, if you already saved your configuration, you might be locked out. [Table 16-2](#) lists the common lockout conditions and how you might recover from them.

**Table 16-2** *CLI Authentication and Command Authorization Lockout Scenarios*

| Feature                                                                                  | Lockout Condition                                                                      | Description                                                                                   | Workaround: Single Mode                                                                                                                                                                                                                                   | Workaround: Multiple Mode                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local CLI authentication                                                                 | No users in the local database                                                         | If you have no users in the local database, you cannot log in, and you cannot add any users.  | Log in and reset the passwords and <b>aaa</b> commands.                                                                                                                                                                                                   | Session into the security appliance from the switch. From the system execution space, you can change to the context and add a user.                                                                                                                                                                                                                                                                                                        |
| TACACS+ command authorization<br>TACACS+ CLI authentication<br>RADIUS CLI authentication | Server down or unreachable and you do not have the fallback method configured          | If the server is unreachable, then you cannot log in or enter any commands.                   | <ol style="list-style-type: none"> <li>1. Log in and reset the passwords and AAA commands.</li> <li>2. Configure the local database as a fallback method so you do not get locked out when the server is down.</li> </ol>                                 | <ol style="list-style-type: none"> <li>1. If the server is unreachable because the network configuration is incorrect on the security appliance, session into the security appliance from the switch. From the system execution space, you can change to the context and reconfigure your network settings.</li> <li>2. Configure the local database as a fallback method so you do not get locked out when the server is down.</li> </ol> |
| TACACS+ command authorization                                                            | You are logged in as a user without enough privileges or as a user that does not exist | You enable command authorization, but then find that the user cannot enter any more commands. | <p>Fix the TACACS+ server user account.</p> <p>If you do not have access to the TACACS+ server and you need to configure the security appliance immediately, then log into the maintenance partition and reset the passwords and <b>aaa</b> commands.</p> | Session into the security appliance from the switch. From the system execution space, you can change to the context and complete the configuration changes. You can also disable command authorization until you fix the TACACS+ configuration.                                                                                                                                                                                            |
| Local command authorization                                                              | You are logged in as a user without enough privileges                                  | You enable command authorization, but then find that the user cannot enter any more commands. | Log in and reset the passwords and <b>aaa</b> commands.                                                                                                                                                                                                   | Session into the security appliance from the switch. From the system execution space, you can change to the context and change the user level.                                                                                                                                                                                                                                                                                             |









# CHAPTER 17

## Configuring Logging

---

The logging feature lets you enable logging and specify how log information is handled. The Log viewing feature lets you view syslog messages in real-time. For a description of the log viewing feature, see [Chapter 45, “Monitoring Logging.”](#)

### About Logging

The security appliance supports the generation of an audit trail of syslog messages that describes its activities (for example, what types of network traffic has been allowed and denied) and enables you to configure system logging.

All syslog messages have a default severity level. You can reassign a message to a new severity level, if necessary. When you choose a severity level, logging messages from that level and lower levels are generated. Messages from a higher level are not included. The higher the severity level, the more messages are included. For more information about logging and syslog messages, see the *Cisco Security Appliance Logging Configuration and System Log Messages*.

### Security Contexts in Logging

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages that you view in your session are only those that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the security appliance to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. To use the device ID, see [Advanced Syslog Configuration, page 17-6](#).

# Using Logging

After you have defined the security context, choose **Configuration > Device Management > Logging**. Under Logging, you can do the following:

- In the Logging Setup pane, enable logging and configure the logging parameters. For more information, see [Logging Setup, page 17-2](#).
- In the Syslog Setup pane, set the facility code to be included in syslog messages that are sent to syslog servers, specify that a timestamp is included in each message, view the severity levels for messages, modify the severity level for messages, and disable messages. For more information, see [Syslog Setup, page 17-4](#).
- In the E-Mail Setup pane, specify syslog messages to be sent by e-mail for notification purposes. For more information, see [Syslog Setup, page 17-4](#).
- In the Event Lists pane, create custom lists of events that specify which messages should be logged; these lists are then used when you set up log filters. For more information, see [Event Lists, page 17-8](#).
- In the Logging Filters pane, specify the criteria that should be used to filter the messages sent to each log destination. The criteria you use for creating filters are severity level, message class, message ID, or events lists. For more information, see [Logging Filters, page 17-10](#).
- In the Rate Limit pane, limit the number of messages that can be generated in a specified time interval. For more information, see [Rate Limit, page 17-14](#).
- In the Syslog Server pane, specify one or more syslog servers to which the security appliance sends syslog messages. For more information, see [Syslog Servers, page 17-16](#).
- In the SMTP pane, specify one or more SMTP servers to which the ASDM sends e-mail alerts and notification messages. For more information, see [SMTP, page 17-17](#).
- In the NetFlow pane, export the information about the progression of a flow of packets. For more information, see [Rate Limit, page 17-14](#).

## Logging Setup

The Logging Setup pane lets you enable system logging on the security appliance and lets you specify general logging parameters, including whether standby units can take over logging, whether to send debug messages, and whether to use the EMBLEM format. This pane also lets you change default settings for the internal log buffer and the security appliance logging queue. To access this pane, choose **Configuration > Device Management > Logging > Logging Setup**.

To configure logging, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Check the <b>Enable logging</b> check box to turn on logging for the main security appliance.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | Check the <b>Enable logging on the failover standby unit</b> check box to turn on logging for the standby security appliance, if available.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 3</b> | Check the <b>Send debug messages as syslogs</b> check box to redirects all debug trace output to system logs. The syslog message does not appear on the console if this option is enabled. Therefore, to view debug messages, you must have logging enabled at the console and have it configured as the destination for the debug syslog message number and severity level. The syslog message number to use is <b>711001</b> . The default severity level for this syslog message is debug. |

- Step 4** Check the **Send syslogs in EMBLEM format** check box to enable EMBLEM format so that it is used for all log destinations, except syslog servers.
- Step 5** In the Buffer Size field, specify the size of the internal log buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, messages will be overwritten unless you save the logs to an FTP server or to internal flash memory. The default buffer size is 4096 bytes. The range is 4096 to 1048576.
- Step 6** To save the buffer content to the FTP server before it is overwritten, check the **Save Buffer To FTP Server** check box. To allow overwriting of the buffer content, uncheck this check box.
- Step 7** Click **Configure FTP Settings** to identify the FTP server and configure the FTP parameters used to save the buffer content. For more information, see [Configure FTP Settings, page 17-3](#).
- Step 8** To save the buffer content to internal flash memory before it is overwritten, check the **Save Buffer To Flash** check box.



**Note** This option is only available in routed or transparent single mode.

- Step 9** Click **Configure Flash Usage** to specify the maximum space to be used in internal flash memory for logging and the minimum free space to be preserved (in KB). Enabling this option creates a directory called “syslog” on the device disk on which messages are stored. For more information, see [Configure Logging Flash Usage, page 17-4](#).



**Note** This option is only available in single, routed or transparent mode.

- Step 10** In the Queue Size field, specify the queue size for system logs that are to be viewed in the security appliance.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configure FTP Settings

The Configure FTP Settings dialog box lets you specify the configuration for the FTP server that is used to save the log buffer content.

To configure FTP settings, perform the following steps:

- Step 1** Check the **Enable FTP client** check box to enable configuration of the FTP client.
- Step 2** In the Server IP Address field, specify the IP address of the FTP server.
- Step 3** In the Path field, specify the directory path on the FTP server to store the saved log buffer content.

- Step 4** In the Username field, specify the username to log in to the FTP server.
- Step 5** In the Password field, specify the password associated with the username to log in to the FTP server.
- Step 6** In the Confirm Password field, reenter the password, and click **OK**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configure Logging Flash Usage

The Configure Logging Flash Usage dialog box lets you specify the limits for saving log buffer content to internal flash memory.

To configure logging flash usage, perform the following steps:

- Step 1** In the Maximum Flash to Be Used by Logging field, specify the maximum amount of internal flash memory that can be used for logging (in KB).
- Step 2** In the Minimum Free Space to Be Preserved field, specify the amount of internal flash memory that is preserved (in KB). When the internal flash memory approaches that limit, new logs are no longer saved.
- Step 3** Click **OK** to close this dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Syslog Setup

The Syslog Setup pane lets you set the facility code to include in messages destined for syslog servers and determine whether syslog messages should include the timestamp. You can change message severity levels and disable messages that you do not want to be logged. To access this pane, choose **Configuration > Device Management > Logging > Syslog Setup**.

To configure system log messaging, perform the following steps:

- Step 1** In the Facility code to include in syslogs drop-down list, specify a system log facility for syslog servers to use as a basis to file messages. The default is LOCAL(4)20, which is what most UNIX systems expect. However, because your network devices share the eight available facilities, you might need to change this value for system logs.
- Step 2** Check the **Include timestamp in syslogs** check box to add the date and time in each syslog message sent.
- Step 3** In the Show drop-down list, choose the information to be displayed in the Syslog ID table. Available options are as follows:
- Choose **Show all syslog IDs** to specify that the Syslog ID table should display the entire list of syslog message IDs.
  - Choose **Show disabled syslog IDs** to specify that the Syslog ID table should display only those syslog message IDs that have been explicitly disabled.
  - Choose **Show syslog IDs with changed logging** to specify that the Syslog ID table should display only those syslog message IDs with severity levels that have changed from their default values.
  - Choose **Show syslog IDs that are disabled or with a changed logging level** to specify that the Syslog ID table should display only those syslog message IDs with severity levels that have been modified and the IDs of syslog messages that have been explicitly disabled.
- Step 4** The Syslog ID Setup Table displays the list of syslog messages based on the setting in the Syslog ID Setup Table. Choose individual messages or ranges of message IDs that you want to modify. You can either disable the selected message IDs or modify their severity levels. To select more than one message ID in the list, click the first ID in the range and Shift-click the last ID in the range.
- Step 5** Click **Advanced** to configure syslog messages to include a device ID. For more information, see [Edit Syslog ID Settings, page 17-5](#) and [Advanced Syslog Configuration, page 17-6](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit Syslog ID Settings

The Edit Syslog ID Settings dialog box lets you modify the severity level of the selected syslog messages or specify that the selected syslog messages should be disabled.

To change syslog message settings, perform the following steps:



### Note

The Syslog ID(s) field is display-only. The values that appear in this area are determined by the entries you chose in the Syslog ID table, located in the Syslog Setup pane.

- Step 1** Check the **Disable Message(s)** check box to disable messages for the syslog message ID(s) displayed in the Syslog ID(s) list.

**Step 2** In the Logging Level drop-down list, choose the severity level of messages to be sent for the syslog message ID(s) displayed in the Syslog ID(s) list. Severity levels are defined as follows:

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

**Step 3** Click **OK** to close this dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Advanced Syslog Configuration

You can configure the security appliance to include a device ID in non-EMBLEM-formatted syslog messages. You can specify only one type of device ID for syslog messages. The device ID can be the hostname of the adaptive security appliance, an interface IP address, the context, or a text string.

The Advanced Syslog Configuration dialog box lets you determine whether syslog messages should include a device ID. If this feature is enabled, the device ID is automatically included in all non-EMBLEM formatted syslog messages.

To specify additional syslog message settings, perform the following steps:

**Step 1** Check the **Enable syslog device ID** check box to specify that a device ID should be included in all non-EMBLEM formatted syslog messages.

**Step 2** To specify which to use as the device ID, choose one of the following options:

- Hostname
- IP address

Choose the interface name that corresponds to the specified IP address from the drop-down list.

- String

In the User-Defined ID field, specify an alphanumeric, user-defined string.

**Step 3** Click **OK** to close this dialog box.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## E-Mail Setup

The E-Mail Setup pane lets you set up a source e-mail address as well as a list of recipients for specified syslog messages to be sent as e-mail messages for notification purposes. You can filter the syslog messages sent to a destination e-mail address by severity level. The table shows which entries have been created. To access this pane, choose **Configuration > Device Management > Logging > E-Mail Setup**.

To configure e-mail to send notification of selected syslog messages, perform the following steps:

- Step 1** In the Source E-Mail Address field, specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.
- Step 2** Click **Add** to enter a new e-mail address recipient of the specified syslog messages.
- Step 3** Choose the severity level of the syslog messages that are sent to the recipient from the drop-down list. The syslog message severity filter used for the destination e-mail address causes messages of the specified severity level and higher to be sent. The global filter specified in the Logging Filters pane is also applied to each e-mail recipient. For more information, see [Logging Filters, page 17-10](#).
- Step 4** Click **Edit** to modify an existing the severity level of the syslog messages that are sent to this recipient.
- Step 5** Click **OK** to close this dialog box.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit E-Mail Recipients

The Add/Edit E-Mail Recipient dialog box lets you set up a destination e-mail address for a specified severity of syslog messages to be sent as e-mail messages.

The severity level used to filter messages for the destination e-mail address is the higher of the severity level specified in this dialog box and the global filter set for all e-mail recipients in the Logging Filters pane.

To add or edit e-mail recipients and severity levels, see [Syslog Setup, page 17-4](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Event Lists

The Event Lists pane lets you create custom lists of events that are used to choose which syslog messages are sent to a specific destination. After you enable logging and configure the logging parameters using the Logging Setup pane, create one or more lists of events on the Event Lists pane. Use these event lists on the Logging Filters pane to specify a logging destination for each list of events. To access this pane, choose **Configuration > Device Management > Logging > Event Lists**.

You use three criteria to define an event list:

- Message Class
- Severity
- Message ID.

A message class is a group of syslog messages related to a security appliance feature that enables you to specify an entire class of messages rather than specifying a class for each message individually. For example, use the auth class to select all syslog messages that are related to user authentication.

Severity level classifies syslog messages based on the relative importance of the event in the normal functioning of the network. The highest severity level is emergency, which means the resource is no longer available. The lowest severity level is debugging, which provides detailed information about every network event.

The message ID is a numeric value that uniquely identifies each message. You can use the message ID in an event list to identify a range of syslog messages, such as 101001-1990120.

To create custom lists of events to send to a specific logging destination, perform the following steps:

- 
- Step 1** Click **Add** to display the Add Event List dialog box.
  - Step 2** In the Name field, enter the name of the event list. No spaces are allowed.
  - Step 3** In the Event Class/Severity area, click **Add** to display the Add Class and Severity Filter dialog box.
  - Step 4** Specify the event class from the drop-down list. Available event classes include the following:
    - All—All event classes
    - auth—User Authentication
    - bridge—Transparent firewall



- ca—PKI Certification Authority
- config—Command Interface
- ha—Failover
- ips—Intrusion Protection Service
- ip—IP Stack
- np—Network Processor
- ospf—OSPF Routing
- rip—RIP Routing
- rm—Resource Manager
- session—User Session
- snmp—SNMP
- sys—System

**Step 5** Specify the severity level from the drop-down list. Severity levels include the following:

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

**Step 6** Click **OK** to close this dialog box.

**Step 7** In the Message ID Filters area, click **Add** to display the Add Syslog Message ID Filter dialog box.

**Step 8** In the Message IDs field, enter a syslog message ID or range of IDs (for example, 101001-199012) to include in the filter.

**Step 9** Click **OK** to close this dialog box.

The event of interest appears in the list. To change this entry, click **Edit**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Event List

The Add/Edit Event List dialog box lets you create or edit an event list that you can use to specify which messages should be sent to a log destination. You can create event lists that filter messages according to message class and severity level, or by message ID.

To add or edit an event list, see [Event Lists, page 17-8](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Syslog Message ID Filter

The Add/Edit Syslog Message ID Filter dialog box lets you specify one or more syslog message IDs to be included in the event list.

To add or edit a syslog message ID filter, see [Event Lists, page 17-8](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Logging Filters

The Logging Filters pane lets you apply message filters to a log destination. Filters applied to a log destination select the messages that are sent to that destination. You can filter messages according to message class and severity level, or use an event list that you can create on the Event Lists pane. To access this pane, choose **Configuration > Device Management > Logging > Logging Filters**.

To apply message filters to a log destination, perform the following steps:

- 
- Step 1** Choose the name of the logging destination to which you want to apply a filter. Available logging destinations are as follows:
- Console
  - Security appliance
  - Syslog Servers

- SNMP Trap
- E-Mail
- Internal Buffer
- Telnet Sessions

Included in this selection are the second column, Syslogs From All Event Classes, and the third column, Syslogs From Specific Event Classes. The second column lists the severity or the event class to use to filter messages for the log destination, or whether logging is disabled for all event classes. The third column lists the event class to use to filter messages for that log destination. For more information, see [Add/Edit Syslog Message ID Filter, page 17-10](#), [Add/Edit Class and Severity Filter, page 17-12](#), and [Event Lists, page 17-8](#).

**Step 2** Click **Edit** to display the Edit Logging Filters dialog box. To apply, edit, or disable filters, see [Edit Logging Filters, page 17-11](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit Logging Filters

The Edit Logging Filters dialog box lets you apply filters to each log destination, edit filters already applied to a log destination, or disable logging from all event classes. You can filter messages according to message class and severity level, or use an event list that you create on the Event Lists pane.

The selected logging destination for this filter appears at the top.

To apply filters, perform the following steps:

- Step 1** Choose the **Filter on severity** option to filter syslog messages according to their severity level.
- Step 2** Choose the **Use event list** option to filter syslog messages according to an event list.
- Step 3** Choose the **Disable logging from all event classes** option to disable all logging to the selected destination.
- Step 4** Click **New** to add a new event list. To add a new event list, see [Event Lists, page 17-8](#).
- Step 5** Specify the event class from the drop-down list. Available event classes include the following:
  - All—All event classes
  - auth—User Authentication
  - bridge—Transparent firewall
  - ca—PKI Certification Authority
  - config—Command Interface

- ha—Failover
- ips—Intrusion Protection Service
- ip—IP Stack
- np—Network Processor
- ospf—OSPF Routing
- rip—RIP Routing
- rm—Resource Manager
- session—User Session
- snmp—SNMP
- sys—System

**Step 6** Specify the level of logging messages from the drop-down list. Severity levels include the following:

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

**Step 7** Click **Add** to add the event class and severity level, and then click **OK**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Class and Severity Filter

The Add/Edit Class and Severity Filter dialog box lets you specify a message class and severity level to be used to filter messages.

To add or edit a message class and severity level for filtering messages, perform the following steps:

**Step 1** Specify the event class from the drop-down list. Available event classes include the following:

- All—All event classes
- auth—User Authentication

- bridge—Transparent firewall
- ca—PKI Certification Authority
- config—Command Interface
- ha—Failover
- ips—Intrusion Protection Service
- ip—IP Stack
- np—Network Processor
- ospf—OSPF Routing
- rip—RIP Routing
- rm—Resource Manager
- session—User Session
- snmp—SNMP
- sys—System

**Step 2** Specify the level of logging messages from the drop-down list. Severity levels include the following:

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

**Step 3** Click **OK** when you are done making selections.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Syslog Message ID Filter

The Add/Edit Syslog Message ID Filter dialog box lets you specify individual syslog message IDs or ranges of IDs to include in the event list filter.

To add or edit a syslog message ID filter, see [Event Lists, page 17-8](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Rate Limit

The Rate Limit pane lets you specify the number of syslog messages that the firewall can send. You can specify a rate limit for message logging levels or limit the rate of a specific message. The rate level is applied to the severity level or to the message ID, not to a destination. Therefore, rate limits affect the volume of messages being sent to all configured destinations. To access this pane, choose **Configuration > Device Management > Logging > Rate Limit**.

To assign rate limits for all syslog messages in a logging level, perform the following steps:

- Step 1** Choose the logging level (message severity level) to which you want to assign rate limits. Severity levels are defined as follows:

| Description   | Severity Level                     |
|---------------|------------------------------------|
| Disabled      | No logging                         |
| Emergency     | 0—System unusable                  |
| Alert         | 1—Immediate action needed          |
| Critical      | 2—Critical condition               |
| Error         | 3—Error condition                  |
| Warning       | 4—Warning condition                |
| Notification  | 5—Normal but significant condition |
| Informational | 6—Informational message only       |
| Debugging     | 7—Debugging only                   |

- Step 2** The No of Messages field displays the number of messages sent. The Interval (Seconds) field displays the interval, in seconds, that is used to limit how many messages at this logging level can be sent. Choose a logging level from the table and click **Edit** to display the Edit Rate Limit for Syslog Logging Level dialog box. To continue, see [Edit Rate Limit for Syslog Logging Level, page 17-15](#).

To assign or change rate limits to individual syslog messages, perform the following steps:

- Step 1** To assign the rate limit of a specific syslog message, click **Add** to display the Add Rate Limit for Syslog Message dialog box. To continue, see [Add/Edit Rate Limit for Syslog Message, page 17-15](#).

- Step 2** To change the rate limit of a specific syslog message, click **Edit** to display the Edit Rate Limit for Syslog Message dialog box. To continue, see [Add/Edit Rate Limit for Syslog Message, page 17-15](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit Rate Limit for Syslog Logging Level

The Edit Rate Limit for Syslog Logging Level **dialog** box lets you limit the number of messages that the adaptive security appliance can send in a specified time interval. The selected message severity level displays.

To change the rate limit of a specified logging level, perform the following steps:

- Step 1** Enter the maximum number of messages at this logging level that can be sent.
- Step 2** Enter the amount of time, in seconds, that is used to limit the rate of messages at this logging level, and click **OK**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Rate Limit for Syslog Message

The Add/Edit Rate Limit for Syslog Message dialog box lets you assign rate limits to a specific syslog message.

To add or change the rate limit for a specific syslog message, perform the following steps:

- Step 1** To add a rate limit to a specific syslog message, click **Add** to display the Add Rate Limit for Syslog Message dialog box. To change a rate limit for a syslog message, click **Edit** to display the Edit Rate Limit for Syslog Message dialog box.
- Step 2** Enter the message ID of the syslog message that you want to limit.

- Step 3** Enter the maximum number of messages that can be sent in the specified time interval.
- Step 4** Enter the amount of time, in seconds, that is used to limit the rate of the specified message, and click **OK**.



**Note** To allow an unlimited number of messages, leave both the Number of Messages and Time Interval fields blank.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Syslog Servers

The Syslog Servers pane lets you specify the syslog servers to which the adaptive security appliance should send syslog messages. To use the syslog server(s) you define, you must enable logging using the Logging Setup pane and set up the available destinations in the Logging Filters pane. To access this pane, choose **Configuration > Device Management > Logging > Syslog Server**.

To specify the syslog servers to which the adaptive security appliance should send syslog messages, perform the following steps:

- Step 1** To add a new syslog server, click **Add** to display the Add Syslog Server dialog box. To change an existing syslog server settings, click **Edit** to display the Edit Syslog Server dialog box.
- Step 2** Specify the number of messages that are allowed to be queued on the adaptive security appliance when a syslog server is busy. A zero value means an unlimited number of messages may be queued.
- Step 3** Check the **Allow user traffic to pass when TCP syslog server is down** check box to specify whether to restrict all traffic if any syslog server is down.
- Step 4** To continue, see [Add/Edit Syslog Server, page 17-17](#).



**Note** You can set up a maximum of four syslog servers per security context (up to a total of 16).

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Syslog Server

The Add/Edit Syslog Server dialog box lets you add or edit the syslog servers to which the adaptive security appliance sends syslog messages. To use the syslog server(s) you define, you must enable logging in the Logging Setup pane and set up the specific filters for log destinations in the Logging Filters pane.

To add or edit a syslog server, perform the following steps:

- 
- Step 1** Choose the interface used to communicate with the syslog server from the drop-down list.
  - Step 2** Enter the IP address that is used to communicate with the syslog server.
  - Step 3** Choose the protocol (either TCP or UDP) that is used by the syslog server to communicate with the security appliance.
  - Step 4** Enter the port number used by the syslog server to communicate with the adaptive security appliance.
  - Step 5** Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).
  - Step 6** Check the **Enable secure logging using SSL/TLS (TCP only)** check box to specify that the connection to the syslog server is secure through the use of SSL/TLS over TCP, and that the syslog message content is encrypted.
  - Step 7** Click **OK** to complete the configuration.
- 

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SMTP

The SMTP pane allows you to configure the remote SMTP server IP address to which e-mail alerts and notifications are sent in response to specific events. To access this pane, choose **Configuration > Device Setup > Logging > SMTP**.

To configure the remote SMTP server, perform the following steps:

- 
- Step 1** Enter the IP address of the primary SMTP server.
- Step 2** (Optional) Enter the IP address of the standby SMTP server, and click **Apply**.
- 

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Using NetFlow

The NetFlow pane lets you enable the transmission of data about a flow of packets. When you enable NetFlow, certain syslog messages become redundant. To maintain system performance, we recommend that you disable all redundant syslog messages, because the same information is exported through NetFlow. To access this pane, choose **Configuration > Device Management > Logging > NetFlow**.

To use NetFlow, perform the following steps:

- 
- Step 1** Enable NetFlow by checking the **Enable the transmission of NetFlow packets** check box.
- If some redundant syslog messages are enabled, the Redundant Syslog dialog box appears. Click **Yes** to disable the redundant syslog messages. Click **No** to leave them unchanged.
- Step 2** Specify the template timeout rate, which is the interval (in minutes) at which template records are sent to all configured destinations (that is, the collector application). The default value is 30 minutes.
- Step 3** Specify the collector(s) to which NetFlow packets will be sent. You can configure a maximum of two collectors. Check the **Configure collector #1** check box to enable the first collector.
- Choose the interface to which NetFlow packets will be sent from the drop-down list.
  - Enter the IP address or hostname and the UDP port number in the associated fields.
- Step 4** If necessary, configure a second collector, and specify the interface details, as you did in the previous step.
- Step 5** Check the **Disable redundant syslog messages** check box to disable all redundant syslog messages. To display the redundant syslog messages and their status, click **Show Redundant Syslog Messages**.
- The Redundant Syslog Messages dialog box appears. The Syslog ID field displays the redundant syslog message numbers. The Disabled field whether the specified syslog message is disabled. Click **OK** to close this dialog box.
- Step 6** To disable individual redundant syslog messages, click **Configuration > Device Management > Logging > Syslog Setup**.
- Step 7** Click **Apply** when you are done making selections.
-

For more information about NetFlow, see the *Cisco Security Appliance Command Line Configuration Guide* and *Implementation Note for NetFlow Collectors*.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |





## **PART 3**

### **Configuring the Firewall**





# CHAPTER 18

## Firewall Mode Overview

---

This chapter describes how the firewall works in each firewall mode. To set the mode at the CLI, see the [“Setting Transparent or Routed Firewall Mode at the CLI”](#) section on page 4-4.



### Note

In multiple context mode, you cannot set the firewall mode separately for each context; you can only set the firewall mode for the entire security appliance.

---

This chapter includes the following sections:

- [Routed Mode Overview, page 18-1](#)
- [Transparent Mode Overview, page 18-1](#)

## Routed Mode Overview

In routed mode, the security appliance is considered to be a router hop in the network. It can use OSPF or RIP (in single context mode). Routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts.

This section includes the following topics:

- [IP Routing Support, page 18-1](#)
- [How Data Moves Through the Security Appliance in Routed Firewall Mode, page 18-1](#)

## IP Routing Support

The security appliance acts as a router between connected networks, and each interface requires an IP address on a different subnet. In single context mode, the routed firewall supports OSPF and RIP. Multiple context mode supports static routes only. We recommend using the advanced routing capabilities of the upstream and downstream routers instead of relying on the security appliance for extensive routing needs.

## How Data Moves Through the Security Appliance in Routed Firewall Mode

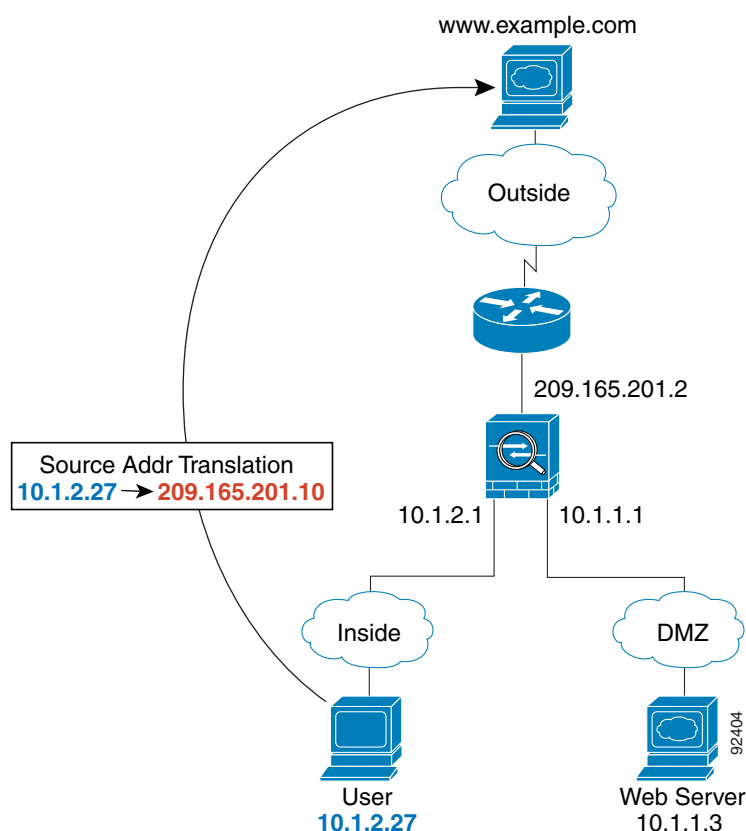
This section describes how data moves through the security appliance in routed firewall mode, and includes the following topics:

- [An Inside User Visits a Web Server, page 18-2](#)
- [An Outside User Visits a Web Server on the DMZ, page 18-3](#)
- [An Inside User Visits a Web Server on the DMZ, page 18-4](#)
- [An Outside User Attempts to Access an Inside Host, page 18-5](#)
- [A DMZ User Attempts to Access an Inside Host, page 18-6](#)

## An Inside User Visits a Web Server

Figure 18-1 shows an inside user accessing an outside web server.

**Figure 18-1** Inside to Outside



The following steps describe how data moves through the security appliance (see [Figure 18-1](#)):

1. The user on the inside network requests a web page from [www.example.com](#).
2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

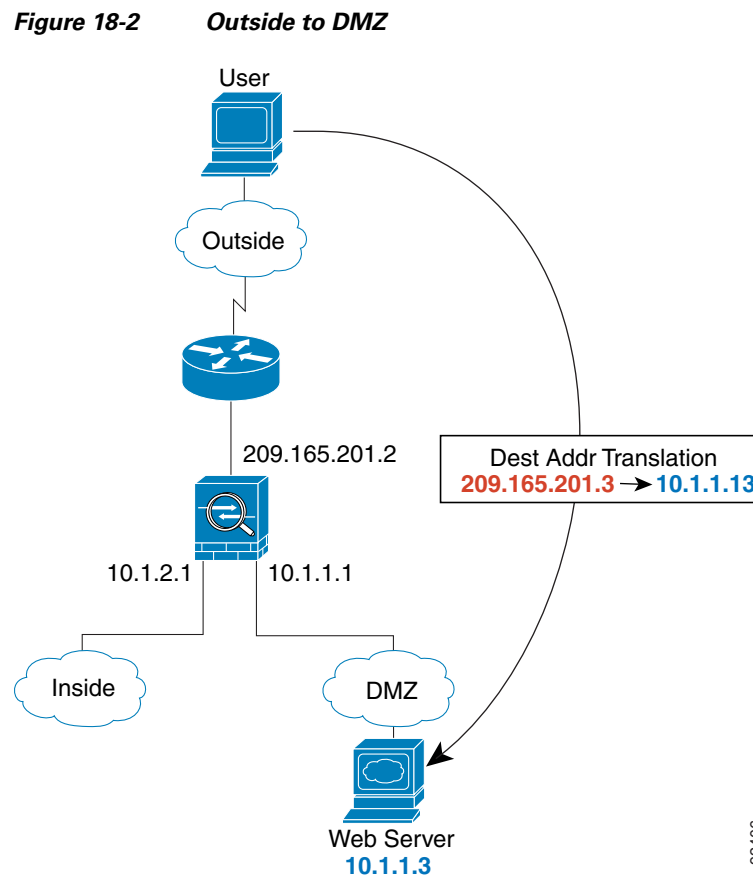
For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface would be unique; the [www.example.com](#) IP address does not have a current address translation in a context.



3. The security appliance translates the local source address (10.1.2.27) to the global address 209.165.201.10, which is on the outside interface subnet.  
The global address could be on any subnet, but routing is simplified when it is on the outside interface subnet.
4. The security appliance then records that a session is established and forwards the packet from the outside interface.
5. When www.example.com responds to the request, the packet goes through the security appliance, and because the session is already established, the packet bypasses the many lookups associated with a new connection. The security appliance performs NAT by translating the global destination address to the local user address, 10.1.2.27.
6. The security appliance forwards the packet to the inside user.

## An Outside User Visits a Web Server on the DMZ

Figure 18-2 shows an outside user accessing the DMZ web server.



The following steps describe how data moves through the security appliance (see Figure 18-2):

1. A user on the outside network requests a web page from the DMZ web server using the global destination address of 209.165.201.3, which is on the outside interface subnet.

2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

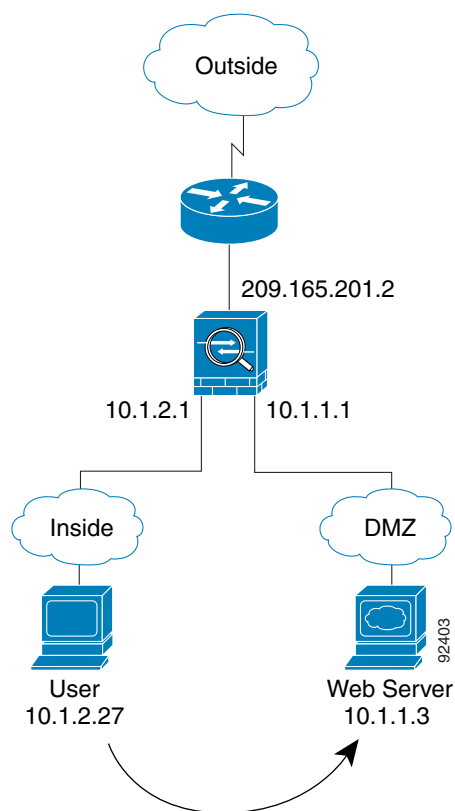
For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the classifier “knows” that the DMZ web server address belongs to a certain context because of the server address translation.

3. The security appliance translates the destination address to the local address 10.1.1.3.
4. The security appliance then adds a session entry to the fast path and forwards the packet from the DMZ interface.
5. When the DMZ web server responds to the request, the packet goes through the security appliance and because the session is already established, the packet bypasses the many lookups associated with a new connection. The security appliance performs NAT by translating the local source address to 209.165.201.3.
6. The security appliance forwards the packet to the outside user.

## An Inside User Visits a Web Server on the DMZ

Figure 18-3 shows an inside user accessing the DMZ web server.

**Figure 18-3** Inside to DMZ



The following steps describe how data moves through the security appliance (see [Figure 18-3](#)):

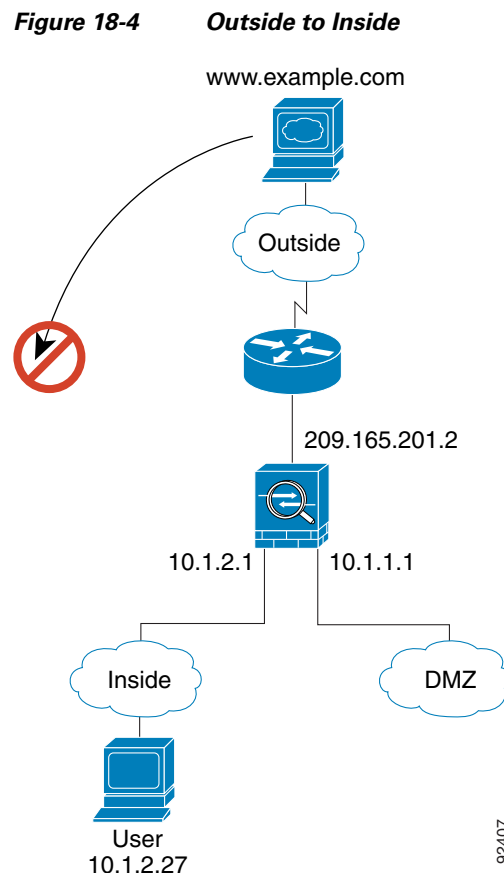
1. A user on the inside network requests a web page from the DMZ web server using the destination address of 10.1.1.3.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface is unique; the web server IP address does not have a current address translation.

3. The security appliance then records that a session is established and forwards the packet out of the DMZ interface.
4. When the DMZ web server responds to the request, the packet goes through the fast path, which lets the packet bypass the many lookups associated with a new connection.
5. The security appliance forwards the packet to the inside user.

## An Outside User Attempts to Access an Inside Host

[Figure 18-4](#) shows an outside user attempting to access the inside network.



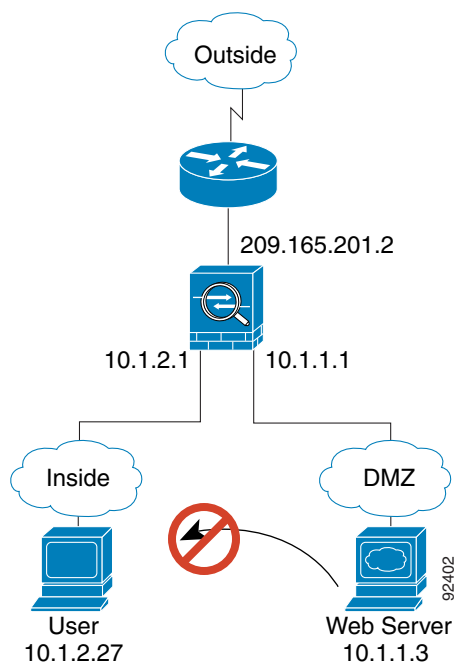
The following steps describe how data moves through the security appliance (see [Figure 18-4](#)):

1. A user on the outside network attempts to reach an inside host (assuming the host has a routable IP address).  
If the inside network uses private addresses, no outside user can reach the inside network without NAT. The outside user might attempt to reach an inside user by using an existing NAT session.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
3. The packet is denied, and the security appliance drops the packet and logs the connection attempt.  
If the outside user is attempting to attack the inside network, the security appliance employs many technologies to determine if a packet is valid for an already established session.

## A DMZ User Attempts to Access an Inside Host

[Figure 18-5](#) shows a user in the DMZ attempting to access the inside network.

**Figure 18-5** DMZ to Inside



The following steps describe how data moves through the security appliance (see [Figure 18-5](#)):

1. A user on the DMZ network attempts to reach an inside host. Because the DMZ does not have to route the traffic on the Internet, the private addressing scheme does not prevent routing.
2. The security appliance receives the packet and because it is a new session, the security appliance verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
3. The packet is denied, and the security appliance drops the packet and logs the connection attempt.

# Transparent Mode Overview

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

This section describes transparent firewall mode, and includes the following topics:

- [Transparent Firewall Network, page 18-2](#)
- [Allowing Layer 3 Traffic, page 18-2](#)
- [Allowed MAC Addresses, page 18-2](#)
- [Passing Traffic Not Allowed in Routed Mode, page 18-2](#)
- [MAC Address vs. Route Lookups, page 18-3](#)
- [Using the Transparent Firewall in Your Network, page 18-4](#)
- [Transparent Firewall Guidelines, page 18-4](#)
- [Unsupported Features in Transparent Mode, page 18-5](#)
- [How Data Moves Through the Transparent Firewall, page 18-11](#)

## Transparent Firewall Network

The security appliance connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network.

## Allowing Layer 3 Traffic

IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. ARPs are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. For Layer 3 traffic travelling from a low to a high security interface, an extended access list is required.

## Allowed MAC Addresses

The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD
- Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

## Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).

**Note**

The transparent mode security appliance does not pass CDP packets or IPv6 packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported.

For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an extended access list. Likewise, protocols like HSRP or VRRP can pass through the security appliance.

Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType access list.

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended access list, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV.

## MAC Address vs. Route Lookups

When the security appliance runs in transparent mode without NAT, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup. Route statements can still be configured, but they only apply to security appliance-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route so the security appliance can reach that subnet.

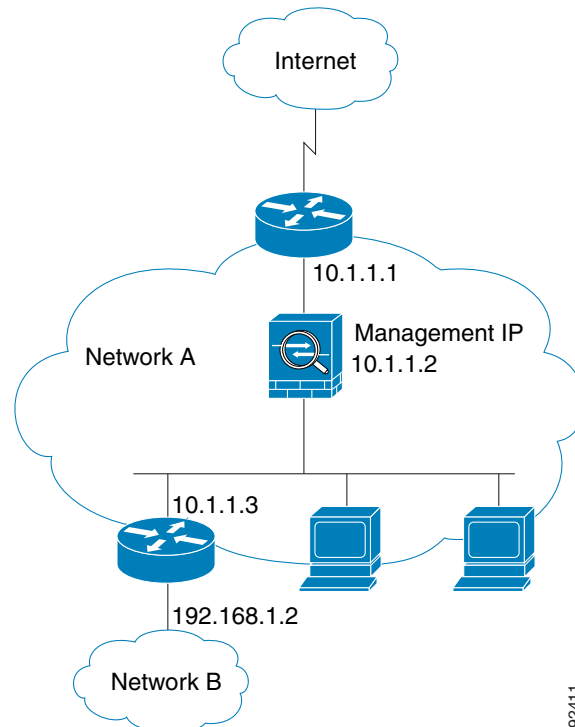
An exception to this rule is when you use voice inspections and the endpoint is at least one hop away from the security appliance. For example, if you use the transparent firewall between a CCM and an H.323 gateway, and there is a router between the transparent firewall and the H.323 gateway, then you need to add a static route on the security appliance for the H.323 gateway for successful call completion.

If you use NAT, then the security appliance uses a route lookup instead of a MAC address lookup. In some cases, you will need static routes. For example, if the real destination address is not directly-connected to the security appliance, then you need to add a static route on the security appliance for the real destination address that points to the downstream router.

## Using the Transparent Firewall in Your Network

Figure 18-1 shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

**Figure 18-6**      **Transparent Firewall Network**



## Transparent Firewall Guidelines

Follow these guidelines when planning your transparent firewall network:

- A management IP address is required; for multiple context mode, an IP address is required for each context.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire device. The security appliance uses this IP address as the source address for packets originating on the security appliance, such as system messages or AAA communications.

The management IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).

You can configure an IP address for the Management 0/0 management-only interface. This IP address can be on a separate subnet from the main management IP address.

- The transparent security appliance uses an inside interface and an outside interface only. If your platform includes a dedicated management interface, you can also configure the management interface or subinterface for management traffic only.

In single mode, you can only use two data interfaces (and the dedicated management interface, if available) even if your security appliance includes more than two interfaces.

- Each directly connected network must be on the same subnet.
- Do not specify the security appliance management IP address as the default gateway for connected devices; devices need to specify the router on the other side of the security appliance as the default gateway.
- For multiple context mode, each context must use different interfaces; you cannot share an interface across contexts.
- For multiple context mode, each context typically uses a different subnet. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

## Unsupported Features in Transparent Mode

Table 18-1 lists the features are not supported in transparent mode.

**Table 18-1**      *Unsupported Features in Transparent Mode*

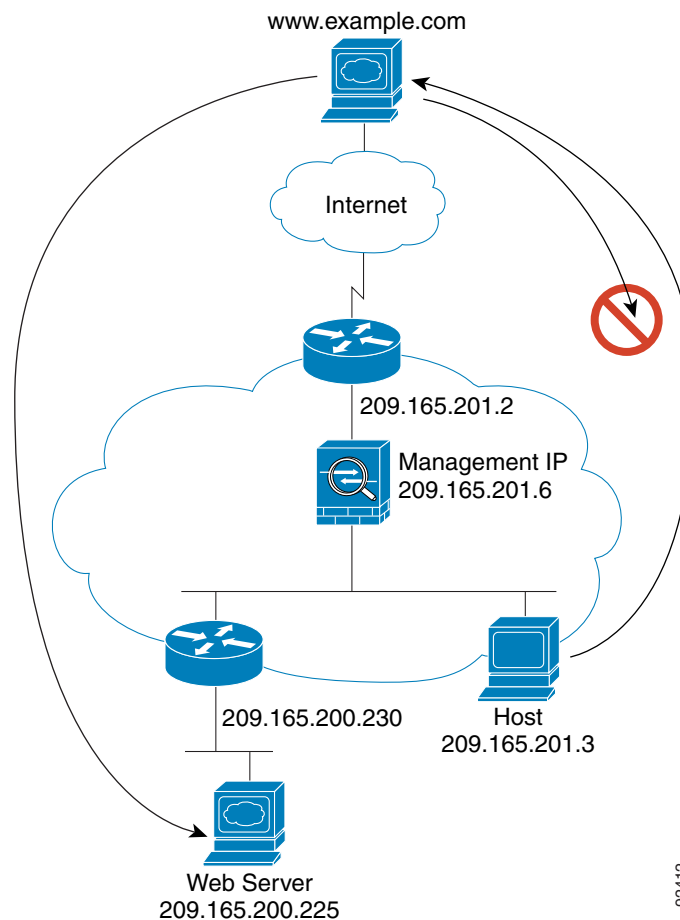
| Feature                             | Description                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic DNS                         | —                                                                                                                                                                                                                                                                                                                                                                    |
| DHCP relay                          | The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through using two extended access lists: one that allows DHCP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.   |
| Dynamic routing protocols           | You can, however, add static routes for traffic originating on the security appliance. You can also allow dynamic routing protocols through the security appliance using an extended access list.                                                                                                                                                                    |
| IPv6                                | You also cannot allow IPv6 using an EtherType access list.                                                                                                                                                                                                                                                                                                           |
| Multicast                           | You can allow multicast traffic through the security appliance by allowing it in an extended access list.                                                                                                                                                                                                                                                            |
| QoS                                 | —                                                                                                                                                                                                                                                                                                                                                                    |
| VPN termination for through traffic | The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the security appliance. You can pass VPN traffic through the security appliance using an extended access list, but it does not terminate non-management connections. Clientless SSL VPN is also not supported. |



## How Data Moves Through the Transparent Firewall

Figure 18-7 shows a typical transparent firewall implementation with an inside network that contains a public web server. The security appliance has an access list so that the inside users can access Internet resources. Another access list lets the outside users access only the web server on the inside network.

**Figure 18-7** Typical Transparent Firewall Data Path



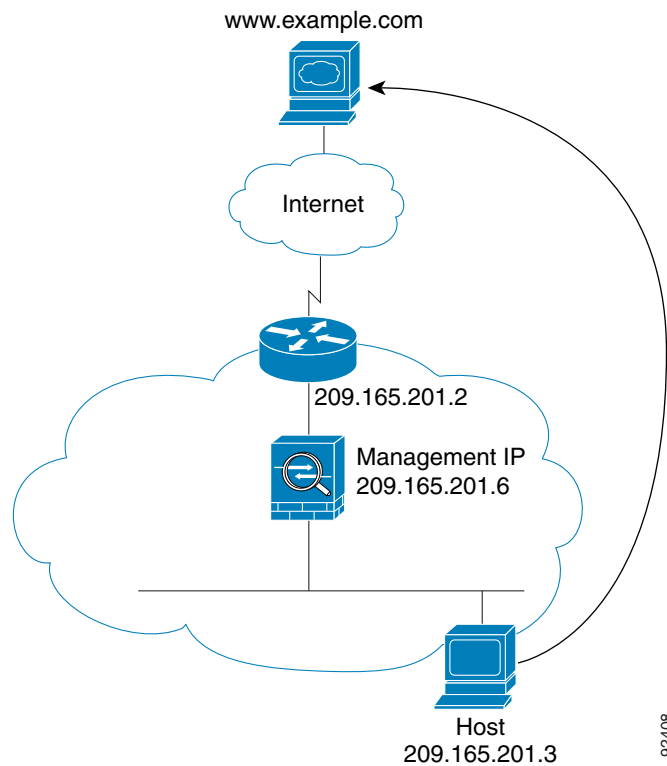
This section describes how data moves through the security appliance, and includes the following topics:

- [An Inside User Visits a Web Server, page 18-12](#)
- [An Inside User Visits a Web Server Using NAT, page 18-13](#)
- [An Outside User Visits a Web Server on the Inside Network, page 18-14](#)
- [An Outside User Attempts to Access an Inside Host, page 18-15](#)

## An Inside User Visits a Web Server

Figure 18-8 shows an inside user accessing an outside web server.

**Figure 18-8** Inside to Outside



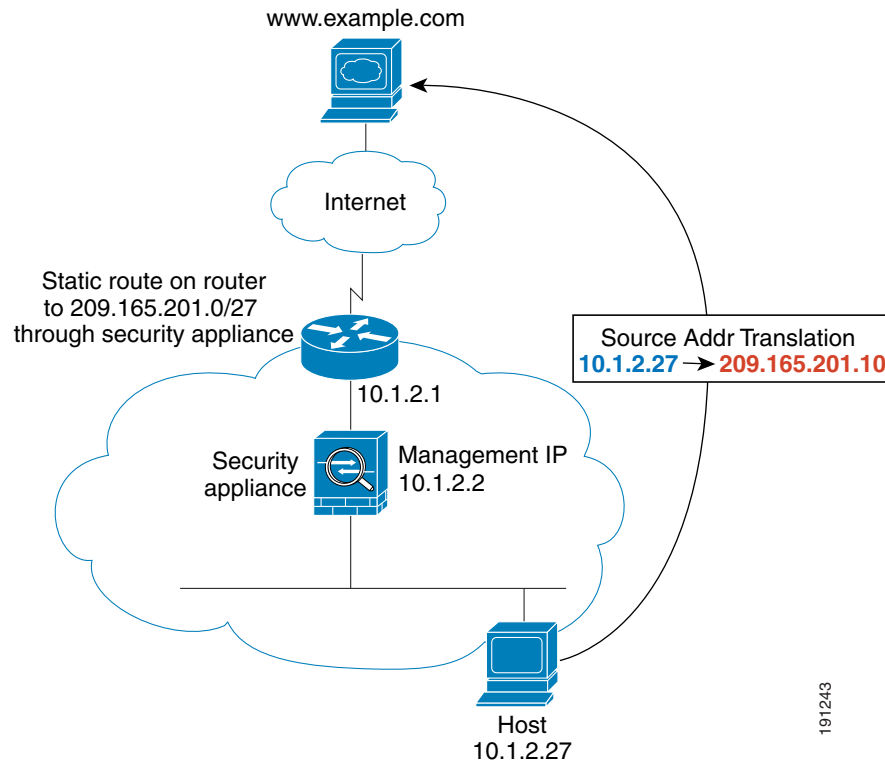
The following steps describe how data moves through the security appliance (see Figure 18-8):

1. The user on the inside network requests a web page from `www.example.com`.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).  
For multiple context mode, the security appliance first classifies the packet according to a unique interface.
3. The security appliance records that a session is established.
4. If the destination MAC address is in its table, the security appliance forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.186.201.2.  
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The security appliance forwards the packet to the inside user.

## An Inside User Visits a Web Server Using NAT

Figure 18-8 shows an inside user accessing an outside web server.

**Figure 18-9**      *Inside to Outside with NAT*



The following steps describe how data moves through the security appliance (see Figure 18-8):

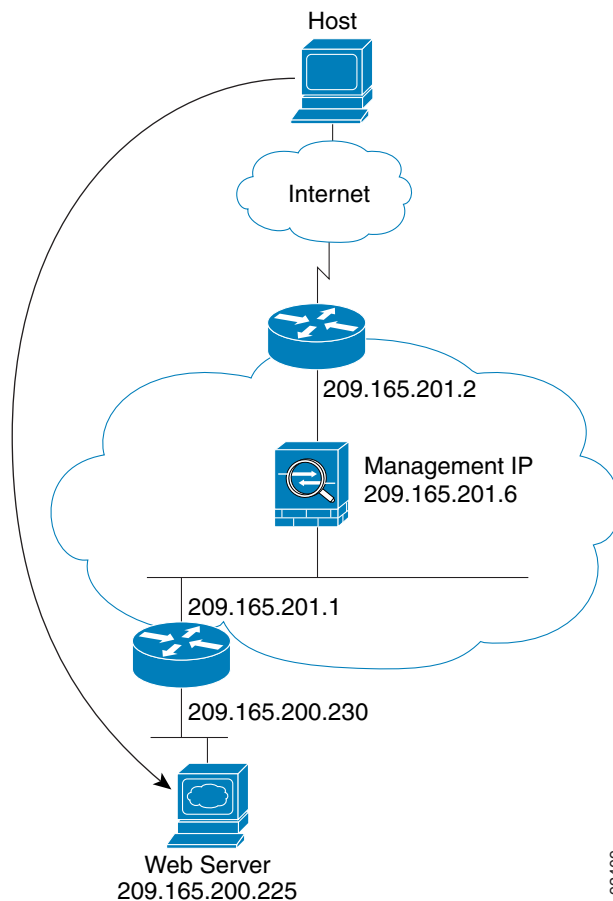
1. The user on the inside network requests a web page from www.example.com.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).  
For multiple context mode, the security appliance first classifies the packet according to a unique interface.
3. The security appliance translates the real address (10.1.2.27) to the mapped address 209.165.201.10. Because the mapped address is not on the same network as the outside interface, then be sure the upstream router has a static route to the mapped network that points to the security appliance.
4. The security appliance then records that a session is established and forwards the packet from the outside interface.
5. If the destination MAC address is in its table, the security appliance forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.165.201.2.  
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
6. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.

7. The security appliance performs NAT by translating the mapped address to the real address, 10.1.2.27.

## An Outside User Visits a Web Server on the Inside Network

Figure 18-10 shows an outside user accessing the inside web server.

**Figure 18-10** Outside to Inside



92409

The following steps describe how data moves through the security appliance (see Figure 18-10):

1. A user on the outside network requests a web page from the inside web server.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).  
For multiple context mode, the security appliance first classifies the packet according to a unique interface.
3. The security appliance records that a session is established.
4. If the destination MAC address is in its table, the security appliance forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 209.186.201.1.

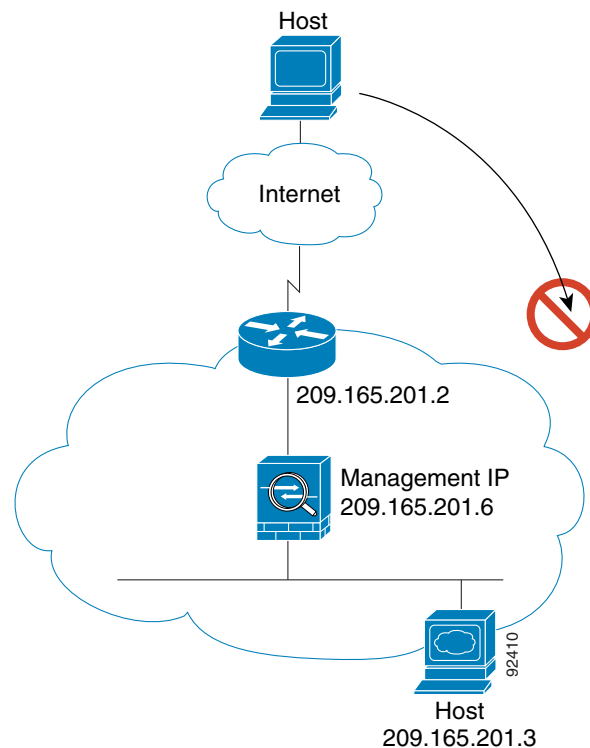
If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The security appliance forwards the packet to the outside user.

## An Outside User Attempts to Access an Inside Host

Figure 18-11 shows an outside user attempting to access a host on the inside network.

**Figure 18-11** Outside to Inside



The following steps describe how data moves through the security appliance (see Figure 18-11):

1. A user on the outside network attempts to reach an inside host.
2. The security appliance receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies if the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the security appliance first classifies the packet according to a unique interface.

3. The packet is denied, and the security appliance drops the packet.
4. If the outside user is attempting to attack the inside network, the security appliance employs many technologies to determine if a packet is valid for an already established session.





# CHAPTER 19

## Adding Global Objects

---

The Objects pane provides a single location where you can configure, view, and modify the reusable components that you need to implement your policy on the security appliance. For example, once you define the hosts and networks that are covered by your security policy, you can select the host or network to which a feature applies, instead of having to redefine it every time. This saves time and ensures consistency and accuracy of your security policy. When you need to add or delete a host or network, you can use the Objects pane to change it in a single place.

This chapter includes the following sections:

- [Using Network Objects and Groups, page 19-1](#)
- [Configuring Service Groups, page 19-5](#)
- [Configuring Class Maps, page 19-8](#)
- [Configuring Inspect Maps, page 19-8](#)
- [Configuring Regular Expressions, page 19-8](#)
- [Configuring TCP Maps, page 19-14](#)
- [Configuring Global Pools, page 19-14](#)
- [Configuring Time Ranges, page 19-15](#)
- [Encrypted Traffic Inspection, page 19-17](#)

## Using Network Objects and Groups

This section describes how to use network objects and groups, and includes the following topics:

- [Network Object Overview, page 19-2](#)
- [Configuring a Network Object, page 19-2](#)
- [Configuring a Network Object Group, page 19-3](#)
- [Using Network Objects and Groups in a Rule, page 19-4](#)
- [Viewing the Usage of a Network Object or Group, page 19-4](#)

## Network Object Overview

Network objects let you predefine host and network IP addresses so that you can streamline subsequent configuration. When you configure the security policy, such as an access rule or a AAA rule, you can choose these predefined addresses instead of typing them in manually. Moreover, if you change the definition of an object, the change is inherited automatically by any rules using the object.

You can add network objects manually, or you can let ASDM automatically create objects from existing configuration, such as access rules and AAA rules. If you edit one of these derived objects, it persists even if you later delete the rule that used it. Otherwise, derived objects only reflect the current configuration if you refresh.

A network object group is a group containing multiple hosts and networks together. A network object group can also contain other network object groups. You can then specify the network object group as the source address or destination address in an access rule.

When you are configuring rules, the ASDM window includes an Addresses side pane at the right that shows available network objects and network object groups; you can add, edit, or delete objects directly in the Addresses pane. You can also drag additional network objects and groups from the Addresses pane to the source or destination of a selected access rule.

## Configuring a Network Object

To configure a network object, perform the following steps:

---

**Step 1** In the Configuration > Firewall > Objects > Network Objects/Group pane, click **Add > Network Object** to add a new object, or choose an object and click **Edit**.

You can also add or edit network objects from the Addresses side pane in a rules window, or when you are adding a rule.

To find an object in the list, enter a name or IP address in the Filter field and click **Filter**. The wildcard characters asterisk (\*) and question mark (?) are allowed.

The Add/Edit Network Object dialog box appears.

**Step 2** Fill in the following values:

- **Name**—(Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- **IP Address**—The IP address, either a host or network address.
- **Netmask**—The subnet mask for the IP address.
- **Description**—(Optional) The description of the network object.

**Step 3** Click **OK**.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.

---

**Note**

You cannot delete a network object that is in use.

---



### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring a Network Object Group

To configure a network object group, perform the following steps:

- 
- Step 1** In the Configuration > Firewall > Objects > Network Objects/Group pane, click **Add > Network Object Group** to add a new object group, or choose an object group and click **Edit**.
- You can also add or edit network object groups from the Addresses side pane in a rules window, or when you are adding a rule.
- To find an object in the list, enter a name or IP address in the Filter field and click Filter. The wildcard characters asterisk (\*) and question mark (?) are allowed.
- The Add/Edit Network Object Group dialog box appears.
- Step 2** In the Group Name field, enter a group name.
- Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- Step 3** (Optional) In the Description field, enter a description up to 200 characters in length.
- Step 4** You can add existing objects or groups to the new group (nested groups are allowed), or you can create a new address to add to the group:
- To add an existing network object or group to the new group, double-click the object in the Existing Network Objects/Groups pane.
- You can also select the object, and then click **Add**. The object or group is added to the right-hand Members in Group pane.
- To add a new address, fill in the values under the Create New Network Object Member area, and click **Add**.
- The object or group is added to the right-hand Members in Group pane. This address is also added to the network object list.
- To remove an object, double-click it in the Members in Group pane, or click **Remove**.
- Step 5** After you add all the member objects, click OK.
- You can now use this network object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.
- 



#### Note

You cannot delete a network object group that is in use.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Using Network Objects and Groups in a Rule

When you create a rule, you can enter an IP address manually, or you can browse for a network object or group to use in the rule. To use a network object or group in a rule, perform the following steps:

- 
- Step 1** From the rule dialog box, click the ... browse button next to the source or destination address field. The Browse Source Address or Browse Destination Address dialog box appears.
- Step 2** You can either add a new network object or group, or choose an existing network object or group by double-clicking it.
- To find an object in the list, enter a name or IP address in the Filter field and click **Filter**. The wildcard characters asterisk (\*) and question mark (?) are allowed.
- To add a new network object, see the [“Configuring a Network Object”](#) section on page 19-2.
  - To add a new network object group, see the [“Configuring a Network Object Group”](#) section on page 19-3.
- After you add a new object or double-click an existing object, it appears in the Selected Source/Destination field. For access rules, you can add multiple objects and groups in the field, separated by commas.
- Step 3** Click **OK**.
- You return to the rule dialog box.
- 

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Viewing the Usage of a Network Object or Group

To view what rules use a network object or group, in the Configuration > Firewall > Objects > Network Objects/Group pane, click the magnifying glass Find icon.

The Usages dialog box appears listing all the rules currently using the network object or group. This dialog box also lists any network object groups that contain the object.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring Service Groups

This section describes how to configure service groups, and includes the following topics:

- [Service Groups, page 19-5](#)
- [Add/Edit Service Group, page 19-6](#)
- [Browse Service Groups, page 19-7](#)

## Service Groups

The Service Groups pane lets you associate multiple services into a named group. You can specify any type of protocol and service in one group or create service groups for each of the following types:

- TCP ports
- UDP ports
- TCP-UDP ports
- ICMP types
- IP protocols

Multiple service groups can be nested into a “group of groups” and used as a single group.

You can use a service group for most configurations that require you to identify a port, ICMP type, or protocol. When you are configuring NAT or security policy rules, the ASDM window even includes a Services pane at the right that shows available service groups and other global objects; you can add, edit, or delete objects directly in the Services pane.

### Fields

- **Add**—Adds a service group. Choose the type of service group to add from the drop-down list or choose Service Group for multiple types.
- **Edit**—Edits a service group.
- **Delete**—Deletes a service group. When a service group is deleted, it is removed from all service groups where it is used. If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.
- **Find**—Filters the display to show only matching names. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.

- Filter field—Enter the name of the service group. The wildcard characters asterisk (\*) and question mark (?) are allowed.
- Filter—Runs the filter.
- Clear—Clears the Filter field.
- Name—Lists the service group names. Click the plus (+) icon next to the name to expand the service group so you can view the services. Click the minus (-) icon to collapse the service group.
- Protocol—Lists the service group protocols.
- Source Ports—Lists the protocol source ports.
- Destination Ports—Lists the protocol destination ports.
- ICMP Type—Lists the service group ICMP type.
- Description—Lists the service group descriptions.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Service Group

The Add/Edit Service Group dialog box lets you assign services to a service group. This dialog box name matches the type of service group you are adding; for example, if you are adding a TCP service group, the Add/Edit TCP Service Group dialog box is shown.

### Fields

- Group Name—Enter the group name, up to 64 characters in length. The name must be unique for all object groups. A service group name cannot share a name with a network object group.
- Description—Enter a description of this service group, up to 200 characters in length.
- Existing Service/Service Group—Identifies items that can be added to the service group. Choose from already defined service groups, or choose from a list of commonly used port, type, or protocol names.
  - Service Groups—The title of this table depends on the type of service group you are adding. It includes the defined service groups.
  - Predefined—Lists the predefined ports, types, or protocols.
- Create new member—Lets you create a new service group member.
  - Service Type—Lets you select the service type for the new service group member. Service types include TCP, UDP, TCP-UDP, ICMP, and protocol.
  - Destination Port/Range—Lets you enter the destination port or range for the new TCP, UDP, or TCP-UDP service group member.

- Source Port/Range—Lets you enter the source port or range for the new TCP, UDP, or TCP-UDP service group member.
- ICMP Type—Lets you enter the ICMP type for the new ICMP service group member.
- Protocol—Lets you enter the protocol for the new protocol service group member.
- Members in Group—Shows items that are already added to the service group.
- Add—Adds the selected item to the service group.
- Remove—Removes the selected item from the service group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Browse Service Groups

The Browse Service Groups dialog box lets you choose a service group. This dialog box is used in multiple configuration screens and is named appropriately for your current task. For example, from the Add/Edit Access Rule dialog box, this dialog box is named “Browse Source Port” or “Browse Destination Port.”

### Fields

- Add—Adds a service group.
- Edit—Edits the selected service group.
- Delete—Deletes the selected service group.
- Find—Filters the display to show only matching names. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
  - Filter field—Enter the name of the service group. The wildcard characters asterisk (\*) and question mark (?) are allowed.
  - Filter—Runs the filter.
  - Clear—Clears the Filter field.
- Type—Lets you choose the type of service group to show, including TCP, UDP, TCP-UDP, ICMP, and Protocol. To view all types, choose **All**. Typically, the type of rule you configure can only use one type of service group; you cannot select a UDP service group for a TCP access rule.
- Name—Shows the name of the service group. Click the plus (+) icon next to the name of an item to expand it. Click the minus (-) icon to collapse the item.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring Class Maps

For information about class maps, see the [“Class Map Field Descriptions”](#) section on page 24-39.

## Configuring Inspect Maps

For information about inspect maps, see the [“Inspect Map Field Descriptions”](#) section on page 24-59.

## Configuring Regular Expressions

This section describes how to configure regular expressions, and includes the following topics:

- [Regular Expressions](#), page 19-8
- [Add/Edit Regular Expression](#), page 19-9
- [Build Regular Expression](#), page 19-11
- [Test Regular Expression](#), page 19-13
- [Add/Edit Regular Expression Class Map](#), page 19-14

## Regular Expressions

Some [Configuring Class Maps](#) and [Configuring Inspect Maps](#) can specify regular expressions to match text inside a packet. Be sure to create the regular expressions before you configure the class map or inspect map, either singly or grouped together in a regular expression class map.

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

### Fields

- Regular Expressions—Shows the regular expressions
  - Name—Shows the regular expression names.
  - Value—Shows the regular expression definitions.
  - Add—Adds a regular expression.
  - Edit—Edits a regular expression.
  - Delete—Deletes a regular expression.
- Regular Expression Classes—Shows the regular expression class maps.

- Name—Shows the regular expression class map name.
- Match Conditions—Shows the match type and regular expressions in the class map.

Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.

Regular Expression—Lists the regular expressions included in each class map.

- Description—Shows the description of the class map.
- Add—Adds a regular expression class map.
- Edit—Edits a regular expression class map.
- Delete—Deletes a regular expression class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Regular Expression

The Add/Edit Regular Expression dialog box lets you define and test a regular expression.

### Fields

- Name—Enter the name of the regular expression, up to 40 characters in length.
- Value—Enter the regular expression, up to 100 characters in length. You can enter the text manually, using the metacharacters in [Table 19-1](#), or you can click **Build** to use the [Build Regular Expression](#) dialog box.



#### Note

As an optimization, the security appliance searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like “http://”, be sure to search for “http:/" instead.

[Table 19-1](#) lists the metacharacters that have special meanings.

**Table 19-1** *regex Metacharacters*

| Character                     | Description               | Notes                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .                             | Dot                       | Matches any single character. For example, <b>d.g</b> matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.                                                                                                                                                                                                                                            |
| ( <i>exp</i> )                | Subexpression             | A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, <b>d(ola)g</b> matches dog and dag, but <b>dolag</b> matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, <b>ab(xy){3}z</b> matches abxyxyxyz. |
|                               | Alternation               | Matches either expression it separates. For example, <b>dog cat</b> matches dog or cat.                                                                                                                                                                                                                                                                                                 |
| ?                             | Question mark             | A quantifier that indicates that there are 0 or 1 of the previous expression. For example, <b>lo?se</b> matches lse or lose.<br><br><b>Note</b> You must enter <b>Ctrl+V</b> and then the question mark or else the help function is invoked.                                                                                                                                           |
| *                             | Asterisk                  | A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, <b>lo*se</b> matches lse, lose, loose, etc.                                                                                                                                                                                                                                      |
| +                             | Plus                      | A quantifier that indicates that there is at least 1 of the previous expression. For example, <b>lo+se</b> matches lose and loose, but not lse.                                                                                                                                                                                                                                         |
| { <i>x</i> } or { <i>x</i> ,} | Minimum repeat quantifier | Repeat at least <i>x</i> times. For example, <b>ab(xy){2,}z</b> matches abxyxyz, abxyxyxyz, and so on.                                                                                                                                                                                                                                                                                  |
| [ <i>abc</i> ]                | Character class           | Matches any character in the brackets. For example, <b>[abc]</b> matches a, b, or c.                                                                                                                                                                                                                                                                                                    |
| [^ <i>abc</i> ]               | Negated character class   | Matches a single character that is not contained within the brackets. For example, <b>[^abc]</b> matches any character other than a, b, or c. <b>[^A-Z]</b> matches any single character that is not an uppercase letter.                                                                                                                                                               |
| [ <i>a-c</i> ]                | Character range class     | Matches any character in the range. <b>[a-z]</b> matches any lowercase letter. You can mix characters and ranges: <b>[abcq-z]</b> matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does <b>[a-cq-z]</b> .<br><br>The dash (-) character is literal only if it is the last or the first character within the brackets: <b>[abc-]</b> or <b>[-abc]</b> .                             |
| ""                            | Quotation marks           | Preserves trailing or leading spaces in the string. For example, “ <b>test</b> ” preserves the leading space when it looks for a match.                                                                                                                                                                                                                                                 |
| ^                             | Caret                     | Specifies the beginning of a line.                                                                                                                                                                                                                                                                                                                                                      |
| \                             | Escape character          | When used with a metacharacter, matches a literal character. For example, <b>\[</b> matches the left square bracket.                                                                                                                                                                                                                                                                    |



**Table 19-1** *regex Metacharacters (continued)*

| Character   | Description                | Notes                                                                                                          |
|-------------|----------------------------|----------------------------------------------------------------------------------------------------------------|
| <i>char</i> | Character                  | When character is not a metacharacter, matches the literal character.                                          |
| <b>\r</b>   | Carriage return            | Matches a carriage return 0x0d.                                                                                |
| <b>\n</b>   | Newline                    | Matches a new line 0x0a.                                                                                       |
| <b>\t</b>   | Tab                        | Matches a tab 0x09.                                                                                            |
| <b>\f</b>   | Formfeed                   | Matches a form feed 0x0c.                                                                                      |
| <b>\xNN</b> | Escaped hexadecimal number | Matches an ASCII character using hexadecimal (exactly two digits).                                             |
| <b>\NNN</b> | Escaped octal number       | Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space. |

- **Build**—Helps you build a regular expression using the [Build Regular Expression](#) dialog box.
- **Test**—Tests a regular expression against some sample text.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Build Regular Expression

The Build Regular Expression dialog box lets you construct a regular expression out of characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.



### Note

As an optimization, the security appliance searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like “http://”, be sure to search for “http:/" instead.

### Fields

**Build Snippet**—This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- **Starts at the beginning of the line (^)**—Indicates that the snippet should start at the beginning of a line, using the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
- **Specify Character String**—Enter a text string manually.

- Character String—Enter a text string.
- Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. For example, if you enter “example.com,” this option converts it to “example\.com”.
- Ignore Case—If you want to match upper and lower case characters, this check box automatically adds text to match both upper and lower case. For example, entering “cats” is converted to “[cC][aA][tT][sS]”.
- Specify Character—Lets you specify a metacharacter to insert in the regular expression.
  - Negate the character—Specifies not to match the character you identify.
  - Any character (.)—Inserts the period (.) metacharacter to match any character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
  - Character set—Inserts a character set. Text can match any character in the set. Sets include:
    - [0-9A-Za-z]
    - [0-9]
    - [A-Z]
    - [a-z]
    - [aeiou]
    - [\n\r\t] (which matches a new line, form feed, carriage return, or a tab)
 For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (upper or lower case) or any digit 0 through 9.
  - Special character—Inserts a character that requires an escape, including \, ?, \*, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.
  - Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
  - Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
  - Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
  - Specified character—Enter any single character.
- Snippet Preview—*Display only*. Shows the snippet as it will be entered in the regular expression.
- Append Snippet—Adds the snippet to the end of the regular expression.
- Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.
- Insert Snippet at Cursor—Inserts the snippet at the cursor.

**Regular Expression**—This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- Selection Occurrences—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is “test me,” and you select “me” and apply **One or more times**, then the regular expression changes to “test (me)+”.
  - Zero or one times (?)—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.

- One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
- Any number of times (\*)—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo\*se** matches lse, lose, loose, etc.
- At least—Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
- Exactly—Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
- Apply to Selection—Applies the quantifier to the selection.
- Test—Tests a regular expression against some sample text.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Test Regular Expression

The Test Regular Expression dialog box lets you test input text against a regular expression to make sure it matches as you intended.

### Fields

- Regular Expression—Enter the regular expression you want to test. By default, the regular expression you entered in the [Add/Edit Regular Expression](#) or [Build Regular Expression](#) dialog box is input into this field. If you change the regular expression during your testing, and click **OK**, the changes are inherited by the [Add/Edit Regular Expression](#) or [Build Regular Expression](#) dialog boxes. Click **Cancel** to dismiss your changes.
- Test String—Enter a text string that you expect to match the regular expression.
- Test—Tests the Text String against the Regular Expression,
- Test Result—*Display only*. Shows if the test succeeded or failed.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Regular Expression Class Map

The Add/Edit Regular Expression Class Map dialog box groups regular expressions together. A regular expression class map can be used by inspection class maps and inspection policy maps.

### Fields

- **Name**—Enter a name for the class map, up to 40 characters in length. The name “class-default” is reserved. All types of class maps use the same name space, so you cannot reuse a name already used by another type of class map.
- **Description**—Enter a description, up to 200 characters in length.
- **Available Regular Expressions**—Lists the regular expressions that are not yet assigned to the class map.
  - **Edit**—Edits the selected regular expression.
  - **New**—Creates a new regular expression.
- **Add**—Adds the selected regular expression to the class map.
- **Remove**—Removes the selected regular expression from the class map.
- **Configured Match Conditions**—Shows the regular expressions in this class map, along with the match type.
  - **Match Type**—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.
  - **Regular Expression**—Lists the regular expression names in this class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring TCP Maps

For information about TCP maps, see the [“Enabling Connection Limits and TCP Normalization” section on page 27-8](#).

## Configuring Global Pools

For information about global pools, see the [“Using Dynamic NAT” section on page 21-16](#).

# Configuring Time Ranges

Use the Time Ranges option to create a reusable component that defines starting and ending times that can be applied to various security features. Once you have defined a time range, you can select the time range and apply it to different options that require scheduling.

The time range feature lets you define a time range that you can attach to traffic rules, or an action. For example, you can attach an access list to a time range to restrict access to the security appliance.

A time range consists of a start time, an end time, and optional recurring entries.



## Note

Creating a time range does not restrict access to the device. This pane defines the time range only.

## Fields

- **Name**—Specifies the name of the time range.
- **Start Time**—Specifies when the time range begins.
- **End Time**—Specifies when the time range ends.
- **Recurring Entries**—Specifies further constraints of active time of the range within the start and stop time specified.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Time Range

The Add/Edit Time Range pane lets you define specific times and dates that you can attach to an action. For example, you can attach an access list to a time range to restrict access to the security appliance. The time range relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.



## Note

Creating a time range does not restrict access to the device. This pane defines the time range only.

## Fields

- **Time Range Name**—Specifies the name of the time range. The name cannot contain a space or quotation mark, and must begin with a letter or number.
- **Start now/Started**—Specifies either that the time range begin immediately or that the time range has begun already. The button label changes based on the Add/Edit state of the time range configuration. If you are adding a new time range, the button displays “Start Now.” If you are editing a time range for which a fixed start time has already been defined, the button displays “Start Now.” When editing a time range for which there is no fixed start time, the button displays “Started.”

- Start at—Specifies when the time range begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Never end—Specifies that there is no end to the time range.
- End at (inclusive)—Specifies when the time range ends. The end time specified is inclusive. For example, if you specified that the time range expire at 11:30, the time range is active through 11:30 and 59 seconds. In this case, the time range expires when 11:31 begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Recurring Time Ranges—Configures daily or weekly time ranges.
  - Add—Adds a recurring time range.
  - Edit—Edits the selected recurring time range.
  - Delete—Deletes the selected recurring time range.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Recurring Time Range

The Add/Edit Recurring Time Range pane lets you fine time ranges further by letting you configure them on a daily or weekly basis.



### Note

Creating a time range does not restrict access to the device. This pane defines the time range only.

### Fields

- Days of the week
  - Every day—Specifies every day of the week.
  - Weekdays—Specifies Monday through Friday.
  - Weekends—Specifies Saturday and Sunday.

- On these days of the week—Lets you choose specific days of the week.
- Daily Start Time—Specifies the hour and the minute that the time range begins.
- Daily End Time (inclusive) area—Specifies the hour and the minute that the time range ends. The end time specified is inclusive.
- Weekly Interval
  - From—Lists the day of the week, Monday through Sunday.
  - Through—Lists the day of the week, Monday through Sunday.
  - Hour—Lists the hour, in the range of 00 through 23.
  - Minute—Lists the minute, in the range of 00 through 59.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Encrypted Traffic Inspection

This section describes how to configure encrypted traffic inspection, and includes the following topics:

- [TLS Proxy, page 19-17](#)
- [Phone Proxy, page 19-24](#)
- [CTL File, page 19-27](#)
- [CTL Provider, page 19-29](#)

## TLS Proxy

For information on how to configure the TLS Proxy, see the following sections:

- [Configure TLS Proxy Pane, page 19-19](#)
- [Adding a TLS Proxy Instance, page 19-20](#)
- [Add TLS Proxy Instance Wizard – Server Configuration, page 19-20](#)
- [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#)
- [Add TLS Proxy Instance Wizard – Other Steps, page 19-23](#)

Use the TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager. Additionally, configure the TLS Proxy on the security appliance to use the following Cisco Unified Communications features:

**Table 19-2** *TLS Proxy Applications and the Security Appliance*

| <b>Application</b>                   | <b>TLS Client</b> | <b>TLS Server</b> | <b>Client Authentication</b> | <b>Security Appliance Server Role</b>                   | <b>Security Appliance Client Role</b>                                                                                  |
|--------------------------------------|-------------------|-------------------|------------------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Mobile Advantage                     | CUMC              | CUMA              | No                           | Using the CUMA private key or certificate impersonation | Any static configured certificate                                                                                      |
| Presence Federation                  | CUP or MS LCS/OCS | CUP or MS LCS/OCS | Yes                          | Proxy certificate, self-signed or by internal CA        | Using the CUP private key or certificate impersonation                                                                 |
| IP Telephone (including Phone Proxy) | IP phone          | CUCM              | Yes                          | Proxy certificate, self-signed or by internal CA        | Local dynamic certificate signed by the security appliance CA (might not need certificate for Phone Proxy application) |

For the Mobility feature, the TLS client is a CUMA client and the TLS server is a CUMA server. The security appliance is between a CUMA client and a CUMA server. The TLS Proxy for CUMA allows the use of an imported PKCS-12 certificate for server proxy during the handshake with the client. CUMA clients are not required to present a certificate (no client authentication) during the handshake. In previous releases, the security appliance required the client to always present a valid certificate and it acted as a private certificate authority (CA) for the clients.

For the Presence Federation feature, the security appliance acts as a TLS Proxy between the Cisco Unified Presence and the foreign server. This allows the security appliance to proxy TLS messages on behalf of the server that initiates the TLS connection, and route the proxied TLS messages to the client. The security appliance stores certificate trustpoints for the server and the client, and presents these certificates on establishment of the TLS session.

The security appliance supports TLS Proxy for various voice applications. For the Phone Proxy feature, the TLS Proxy running on the security appliance has the following key features:

- The TLS Proxy is implemented on the security appliance to intercept the TLS signaling from IP phones.
- The TLS Proxy decrypts the packets, sends packets to the inspection engine for NAT rewrite and protocol conformance, optionally encrypts packets, and sends them to CUCM or sends them in clear text if the IP phone is configured to be in nonsecure mode on the CUCM.
- The TLS Proxy is a transparent proxy that works based on establishing trusted relationship between the TLS client, the proxy (the security appliance), and the TLS Server.



## Configure TLS Proxy Pane

You can configure the TLS Proxy from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane. For a detailed overview of the TLS Proxy, see [TLS Proxy, page 19-17](#).

Configuring a TLS Proxy lets you use the TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and enable the security appliance for the Cisco Unified Communications features:

- TLS Proxy for the Cisco Unified Presence Server (CUPS), part of Presence Federation
- TLS Proxy for the Cisco Unified Mobility Advantage (CUMA) server, part of Mobile Advantage
- Phone Proxy

### Fields

- TLS Proxy Name—Lists the TLS Proxy name.
- Server Proxy Certificate—Lists the trustpoint, which is either self-signed or enrolled with a certificate server.
- Local Dynamic Certificate Issuer—Lists the local certificate authority to issue client or server dynamic certificates.
- Client Proxy Certificate—Lists the proxy certificate for the TLS client. The security appliance uses the client proxy certificate to authenticate the TLS client during the handshake between the proxy and the TLS client. The certificate can be either self-signed, enrolled with a certificate authority, or issued by the third party.
- Add—Adds a TLS Proxy by launching the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#) for the steps to create a TLS Proxy instance.
- Edit—Edits a TLS Proxy. The fields in the Edit panel area identical to the fields displayed when you add a TLS Proxy instance. See [Add TLS Proxy Instance Wizard – Server Configuration, page 19-20](#) and [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).
- Delete—Deletes a TLS Proxy.
- Maximum Sessions—Lets you specify the maximum number of TLS Proxy sessions to support.
  - Specify the maximum number of TLS Proxy sessions that the ASA needs to support. By default, the ASA supports 100 sessions.
  - Maximum number of sessions—The minimum is 1. The maximum is dependent on the platform. The default is 100.



#### Note

The maximum number of sessions is global to all TLS proxy sessions.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Adding a TLS Proxy Instance

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy, page 19-17](#).

This wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

**Step 1** Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

**Step 2** To add a new TLS Proxy Instance, click **Add**.

The Add TLS Proxy Instance Wizard opens.

**Step 3** In the TLS Proxy Name field, type the TLS Proxy name.

**Step 4** Click **Next**.

The Add TLS Proxy Instance Wizard – Server Configuration dialog box opens. In this step of the wizard, configure the server proxy parameters for original TLS Server—the Cisco Unified Call Manager (CUCM) server, the Cisco Unified Presence Server (CUPS), or the Cisco Unified Mobility Advantage (CUMA) server. See [Add TLS Proxy Instance Wizard – Server Configuration, page 19-20](#).

After configuring the server proxy parameters, the wizard guides you through configuring client proxy parameters (see [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#)) and provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-23](#)).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add TLS Proxy Instance Wizard – Server Configuration

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy, page 19-17](#).

The fields in the Edit TLS Proxy dialog box are identical to the fields displayed when you add a TLS Proxy instance. Use the Edit TLS Proxy – Server Configuration tab to edit the server proxy parameters for the original TLS Server—the Cisco Unified Call Manager (CUCM) server, the Cisco Unified Presence Server (CUPS), or the Cisco Unified Mobility Advantage (CUMA) server.

The Add TLS Proxy Instance Wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

- 
- Step 1** Complete the first step of the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#).
- The Add TLS Proxy Instance Wizard – Server Configuration dialog box opens.
- Step 2** Specify the server proxy certificate by doing one of the following:
- To add a new certificate, click **Manage**. The Manage Identify Certificates dialog box opens. See [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).
  - To select an existing certificate, select one from the drop-down list.
- The server proxy certificate is used to specify the trustpoint to present during the TLS handshake. The trustpoint can be self-signed or enrolled locally with the certificate service on the proxy. For example, for the Phone Proxy, the server proxy certificate is used by the Phone Proxy during the handshake with the IP phones.
- When you are configuring the TLS Proxy for the Phone Proxy, select the certificate that has a filename beginning with **\_internal\_PP\_**. When you create the CTL file for the Phone Proxy, the security appliance, creates an internal trustpoint used by the Phone Proxy to sign the TFTP files. The trustpoint is named **\_internal\_PP\_ctl-instance\_filename**.
- When the Phone Proxy is operating in a mixed-mode CUCM cluster, you must import the CUCM certificate by clicking **Add** in the Manage Identify Certificates dialog box. See [Add/Install an Identity Certificate, page 33-7](#).
- Step 3** To install the TLS server certificate in the security appliance trust store, so that the security appliance can authenticate the TLS server during TLS handshake between the proxy and the TLS server, click **Install TLS Server's Certificate**.
- The Manage CA Certificates dialog box opens. See [CA Certificate Authentication, page 33-1](#). Click **Add** to open the Install Certificate dialog box. See [Add/Install a CA Certificate, page 33-2](#).
- When you are configuring the TLS Proxy for the Phone Proxy, click **Install TLS Server's Certificate** and install the Cisco Unified Call Manager (CUCM) certificate so that the proxy can authenticate the IP phones on behalf of the CUCM server.
- Step 4** To require the security appliance to present a certificate and authenticate the TLS client during TLS handshake, check the Enable client authentication during TLS Proxy handshake check box.
- When adding a TLS Proxy Instance for Mobile Advantage (the CUMC client and CUMA server), disable the check box when the client is incapable of sending a client certificate.
- See [TLS Proxy, page 19-17](#) to determine which TLS clients used by the Cisco Unified Communication features are capable of client authentication.
- Step 5** Click **Next**.
- The Add TLS Proxy Instance Wizard – Client Configuration dialog box opens. In this step of the wizard, configure the client proxy parameters for original TLS Client—the CUMC client for Mobile Advantage, CUP or MS LCS/OCS client for Presence Federation, or the IP phone for the Phone Proxy. See [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).
- After configuring the client proxy parameters, the wizard provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-23](#)).
-

## Add TLS Proxy Instance Wizard – Client Configuration

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy, page 19-17](#).

The fields in the Edit TLS Proxy dialog box are identical to the fields displayed when you add a TLS Proxy instance. Use the Edit TLS Proxy – Client Configuration tab to edit the client proxy parameters for the original TLS Client, such as IP phones, CUMA clients, the Cisco Unified Presence Server (CUPS), or the Microsoft OCS server.

This wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

**Step 1** Complete the first two steps of the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#) and [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).

The Add TLS Proxy Instance Wizard – Client Configuration dialog box opens.

**Step 2** To specify a client proxy certificate to use for the TLS Proxy, perform the following. Select this option when the client proxy certificate is being used between two servers; for example, when configuring the TLS Proxy for Presence Federation, which uses the Cisco Unified Presence Server (CUPS), both the TLS client and TLS server are both servers.

- a. Check the Specify the proxy certificate for the TLS Client... check box.
- b. Select a certificate from the drop-down list.

Or

To create a new client proxy certificate, click **Manage**. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-6](#).



### Note

When you are configuring the TLS Proxy for the Phone Proxy and it is using the mixed security mode for the CUCM cluster, you must configure the LDC Issuer. The LDC Issuer lists the local certificate authority to issue client or server dynamic certificates.

**Step 3** To specify an LDC Issuer to use for the TLS Proxy, perform the following. When you select and configure the LDC Issuer option, the security appliance acts as the certificate authority and issues certificates to TLS clients.

- a. Click the Specify the internal Certificate Authority to sign the local dynamic certificate for phones... check box.
- b. Click the Certificates radio button and select a self-signed certificate from the drop-down list or click **Manage** to create a new LDC Issuer. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-6](#).

Or

Click the Certificate Authority radio button to specify a Certificate Authority (CA) server. When you specify a CA server, it needs to be created and enabled in the security appliance. To create and enable the CA server, click **Manage**. The Edit CA Server Settings dialog box opens. See [Local Certificate Authority, page 33-12](#).

**Note**

To make configuration changes after the local certificate authority has been configured for the first time, disable the local certificate authority.

- c. In the Key-Pair Name field, select a key pair from the drop-list. The list contains the already defined RSA key pair used by client dynamic certificates. To see the key pair details, including generation time, usage, modulus size, and key data, click **Show**.

Or

To create a new key pair, click **New**. The Add Key Pair dialog box opens. See [Add/Install an Identity Certificate, page 33-7](#) for details about the Key Pair fields.

- Step 4** In the Security Algorithms area, specify the available and active algorithms to be announced or matched during the TLS handshake.

- Available Algorithms—Lists the available algorithms to be announced or matched during the TLS handshake: des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, and null-sha1.

Add—Adds the selected algorithm to the active list.

Remove—Removes the selected algorithm from the active list.

- Active Algorithms—Lists the active algorithms to be announced or matched during the TLS handshake: des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, and null-sha1. For client proxy (acting as a TLS client to the server), the user-defined algorithms replace the original ones from the hello message for asymmetric encryption method between the two TLS legs. For example, the leg between the proxy and Call Manager may be NULL cipher to offload the Call Manager.

Move Up—Moves an algorithm up in the list.

Move Down—Moves an algorithm down in the list.

- Step 5** Click **Next**.

The Add TLS Proxy Instance Wizard – Other Steps dialog box opens. The Other Steps dialog box provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-23](#)).

## Add TLS Proxy Instance Wizard – Other Steps

The last dialog box of the Add TLS Proxy Instance Wizard specifies the additional steps required to make TLS Proxy fully functional. In particular, you need to perform the following tasks to complete the TLS Proxy configuration:

- Export the local CA certificate or LDC Issuer and install them on the original TLS server.  
To export the LDC Issuer, go to Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Export. See [Export an Identity Certificate, page 33-9](#).
- For the TLS Proxy, enable Skinny and SIP inspection between the TLS server and TLS clients. See [SIP Inspection, page 24-21](#) and [Skinny \(SCCP\) Inspection, page 24-22](#). When you are configuring the TLS Proxy for Presence Federation (which uses CUP), you only enable SIP inspection because the feature supports only the SIP protocol.
- For the TLS Proxy for CUMA, enable MMP inspection. See [MMP Inspection, page 24-17](#).
- When using the internal Certificate Authority of the security appliance to sign the LDC Issuer for TLS clients, perform the following:

- Use the Cisco CTL Client to add the server proxy certificate to the CTL file and install the CTL file on the security appliance.

For information on the Cisco CTL Client, see “Configuring the Cisco CTL Client” in *Cisco Unified CallManager Security Guide*.

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/security/5\\_0\\_4/secuauth.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/5_0_4/secuauth.html)

To install the CTL file on the security appliance, go to Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL Provider > Add. The Add CTL Provider dialog box opens. For information on using this dialog box to install the CTL file, see [Add/Edit CTL Provider, page 19-30](#).

- Create a CTL provider instance for connections from the CTL clients. See [Add/Edit CTL Provider, page 19-30](#).

## Phone Proxy

For information on how to configure the Phone Proxy, see the following sections:

- [Configuring the Phone Proxy, page 19-24](#)
- [Add/Edit TFTP Server, page 19-26](#)

Use the Phone Proxy to configure a Phone Proxy between a Call Manager and IP phones. If the Phone Proxy is configured, the security appliance encrypts signaling connections from IP phones in the untrusted networks and sends them in the clear to the CUCM on a trusted network.

## Configuring the Phone Proxy

Configuring the Phone Proxy requires the following steps:

Step 1: Create the CTL file. See [Creating a CTL File, page 19-28](#).

Step 2: Create the TLS Proxy instance to handle the encrypted signaling. See [Adding a TLS Proxy Instance, page 19-20](#).

Step 3: Create the Phone Proxy instance. See [Creating a Phone Proxy Instance, page 19-24](#).

Step 4: Enable the Phone Proxy with SIP and Skinny inspection. See [SIP Inspection, page 24-21](#) and [Skinny \(SCCP\) Inspection, page 24-22](#).

## Creating a Phone Proxy Instance

Use the Configure Phone Proxy pane to add a Phone Proxy. For a detailed overview of the Phone Proxy used by the security appliance, see [Phone Proxy, page 19-24](#).

This pane is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Phone Proxy pane.

- 
- |               |                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Phone Proxy pane.              |
| <b>Step 2</b> | Check the Enable Phone Proxy check box to enable the feature.                                                |
| <b>Step 3</b> | In the Media Termination Address field, type the IP address to use for media connections to the Phone Proxy. |

Specify the virtual IP address that will be created for the Phone Proxy to use during media termination. Only one virtual interface can be configured per Phone Proxy instance. The Phone Proxy inserts the media termination IP address into the media address portion of the signaling messages.

The security appliance must have an IP address for media termination that meets the following criteria:

- The IP address is a publicly routable address that is an unused IP address on an attached network to the security appliance interface that will never be used by another device in your network.
- The IP address cannot be the same as the security appliance interface IP address. Specifically, it cannot be the same as the least secure interface on the security appliance.
- The IP address cannot overlap with existing static NAT rules.
- The IP address cannot be the same as the CUCM or TFTP server IP address.
- Add routes to the other interfaces so that IP phones on other interfaces can reach the media termination address.

**Step 4** Specify the TLS Proxy by doing one of the following:

- To add a new TLS Proxy Instance, click **Manage**. The Configure TLS Proxy dialog box opens. See [Configure TLS Proxy Pane, page 19-19](#).
- To select an existing TLS Proxy, select one from the drop-down list.

**Step 5** In the TFTP Server Settings list, do one of the following:

- To add a new TFTP server for the Phone Proxy, click **Add**. The Add TFTP Server dialog box opens. See [Add/Edit TFTP Server, page 19-26](#).
- To select an existing TFTP server, select one from the drop-down list.



**Note**

The TFTP server must reside on the same interface as the Cisco Unified Call Manager. Additionally, If NAT is configured for the TFTP server, the NAT configuration must be configured prior to configuring the specifying the TFTP server while creating the Phone Proxy instance.

**Step 6** Specify the CTL File to use for the Phone Proxy by doing one of the following:

- To use an existing CTL File, check the Use the Certificate Trust List File generated by the CTL instance check box.
- To create a new CTL file for the Phone Proxy, click the link Generate Certificate Trust List File. The Create a Certificate Trust List (CTL) File pane opens. See [Creating a CTL File, page 19-28](#).

**Step 7** To specify the security mode of the CUCM cluster, click one of the following options in the CUCM Cluster Mode field:

- Non-secure—Specifies the cluster mode to be in nonsecure mode when configuring the Phone Proxy feature.
- Mixed—Specifies the cluster mode to be in mixed mode when configuring the Phone Proxy feature.

**Step 8** To configure the idle timeout after which the secure-phone entry is removed from the Phone Proxy database (the default is 5 minutes), enter a value in the format *hh:mm:ss*.

Since secure phones always request a CTL file upon bootup, the Phone Proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout. The entry timestamp is updated for each registration refresh the Phone Proxy receives for SIP phones and KeepAlives for SCCP phones.

Specify a value that is greater than the maximum timeout value for SCCP KeepAlives and SIP Register refresh. For example, if the SCCP KeepAlives are configured for 1 minute intervals and the SIP Register Refresh is configured for 3 minutes, configure this timeout value greater than 3 minutes.

- Step 9** To preserve Call Manager configuration on the IP phones, check the Preserve the Call Manager's configuration on the phone... When this option is unchecked, the following service settings are disabled on the IP phones:
- PC Port
  - Gratuitous ARP
  - Voice VLAN access
  - Web Access
  - Span to PC Port
- Step 10** To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, do the following:
- a. Check the Configure a http-proxy which would be written into the phone's config file... check box.
  - b. In the IP Address field, type the IP address of the HTTP proxy and the listening port of the HTTP proxy.  
  
The IP address you enter should be the global IP address based on where the IP phone and HTTP proxy server is located. You can enter a hostname in the IP Address field when that hostname can be resolved to an IP address by the security appliance (for example, DNS lookup is configured) because the security appliance will resolve the hostname to an IP address. If a port is not specified, the default will be 8080.
  - c. In the Interface field, select the interface on which the HTTP proxy resides on the security appliance.
- Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.
- Step 11** To force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario, check the Enable CIPC security mode authentication check box.
- Because CIPC requires an LSC to perform the TLS handshake, CIPC needs to register with the CUCM in nonsecure mode using cleartext signaling. To allow the CIPC to register, create an ACL that allows the CIPC to connect to the CUCM on the nonsecure SIP/SCCP signaling ports (5060/2000).
- CIPC uses a different cipher when doing the TLS handshake and requires the null-sha1 cipher and SSL encryption be configured. To add the null-sha1 cipher, go to Configuration > Device Management > Advanced > SSL Settings > Encryption section. Select the null-sha1 SSL encryption type and add it to the Available Algorithms.
- Current versions of Cisco IP Communicator (CIPC) support authenticated mode and perform TLS signaling but not voice encryption.
- Step 12** Click **Apply** to save the Phone Proxy configuration settings.
- 

## Add/Edit TFTP Server

Use the Add/Edit TFTP Server dialog box to specify the IP address of the TFTP server and the interface on which the TFTP server resides.

The Phone Proxy must have at least one CUCM TFTP server configured. Up to five TFTP servers can be configured for the Phone Proxy.



The TFTP server is assumed to be behind the firewall on the trusted network; therefore, the Phone Proxy intercepts the requests between the IP phones and TFTP server.

**Note**

If NAT is configured for the TFTP server, the NAT configuration must be configured prior to specifying the TFTP server while creating the Phone Proxy instance.

**Fields**

**TFTP Server IP Address**—Specifies the address of the TFTP server. Create the TFTP server using the actual internal IP address.

**Port**—(Optional) Specifies the port the TFTP server is listening in on for the TFTP requests. This should be configured if it is not the default TFTP port 69.

**Interface**—Specifies the interface on which the TFTP server resides. The TFTP server must reside on the same interface as the Cisco Unified Call Manager (CUCM).

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## CTL File

For information on how to configure CTL files, see the following sections:

- [Creating a CTL File, page 19-28](#)
- [Add/Edit Record Entry, page 19-28](#)
- [CTL Provider, page 19-29](#)

Create a Certificate Trust List (CTL) file that is required by the Phone Proxy. Specify the certificates needed by creating a new CTL file or by specifying the path of an exiting CTL file to parse from Flash memory.

Create trustpoints and generate certificates for each entity in the network (CUCM, CUCM and TFTP, TFTP server, CAPF) that the IP phones must trust. The certificates are used in creating the CTL file. You need to create trustpoints for each CUCM (primary and secondary if a secondary CUCM is used) and TFTP server in the network. The trustpoints need to be in the CTL file for the phones to trust the CUCM.

Create the CTL File that will be presented to the IP phones during the TFTP. The address must be the translated or global address of the TFTP server or CUCM if NAT is configured.

When the file is created, it creates an internal trustpoint used by the Phone Proxy to sign the TFTP files. The trustpoint is named `_internal_PP_ctl-instance_filename`.

## Creating a CTL File

Use the Create a Certificate Trust List (CTL) File pane to create a CTL file for the Phone Proxy. This pane creates the CTL file that is presented to the IP phones during the TFTP handshake with the security appliance. For a detailed overview of the CTL file used by the Phone Proxy, see [CTL File, page 19-27](#).

The Create a Certificate Trust List (CTL) File pane is used to configure the attributes for generating the CTL file. The name of the CTL file instance is generated by the ASDM. When the user tries to edit the CTL file instance configuration, the ASDM automatically generates the **shutdown** CLI command first and the **no shutdown** CLI command as the last command.

This pane is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL File pane.

- 
- Step 1** Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL File pane.
- Step 2** Check the Enable Certificate Trust List File check box to enable the feature.
- Step 3** To specify the CTL file to use for the Phone Proxy, perform one of the following:
- If there is an existing CTL file available, download the CTL file to Flash memory by using the File Management Tool in the ASDM Tools menu. Select the Use certificates present in the CTL stored in flash radio button and specify the CTL file name and path in the text box.  
  
Use an existing CTL file to install the trustpoints for each entity in the network (CUCM, CUCM and TFTP, TFTP server, CAPF) that the IP phones must trust. If you have an existing CTL file that contains the correct IP addresses of the entities (namely, the IP address that the IP phones use for the CUCM or TFTP servers), you can use it to create a new CTL file. Store a copy of the existing CTL file to Flash memory and rename it something other than `CTLFile.tlv`.
  - If there is no existing CTL file available, select Create new CTL file radio button.  
  
Add Record entries for each entity in the network such as CUCM, TFTP, and CUCM-TFTP option by clicking **Add**. The Add Record Entry dialog box opens. See [Add/Edit Record Entry, page 19-28](#).
- Step 4** Specify the number SAST certificate tokens required. The default is 2. maximum allowed is 5.  
  
Because the Phone Proxy generates the CTL file, it needs to create the System Administrator Security Token (SAST) key to sign the CTL file itself. This key can be generated on the security appliance. A SAST is created as a self-signed certificate. Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.
- Step 5** Click **Apply** to save the CTL file configuration settings.
- 

## Add/Edit Record Entry

Use the Add/Edit Record Entry dialog box to specify the trustpoints to be used for the creation of the CTL file.

Add additional record-entry configurations for each entity that is required in the CTL file.

### Fields

Type—Specifies the type of trustpoint to create:

- `cucm`: Specifies the role of this trustpoint to be CCM. Multiple CCM trustpoints can be configured.

- **cucm-tftp:** Specifies the role of this trustpoint to be CCM+TFTP. Multiple CCM+TFTP trustpoints can be configured.
- **tftp:** Specifies the role of this trustpoint to be TFTP. Multiple TFTP trustpoints can be configured.
- **capf:** Specifies the role of this trustpoint to be CAPF. Only one CAPF trustpoint can be configured.

**Address**—Specifies the IP address of the trustpoint. The IP address you specify must be the global address of the TFTP server or CUCM if NAT is configured. The global IP address is the IP address as seen by the IP phones because it will be the IP address used for the CTL record for the trustpoint.

**Certificate**—Specifies the Identity Certificate for the record entry in the CTL file. You can create a new Identity Certificate by clicking **Manage**. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-6](#).

You can add an Identity Certificate by generating a self-signed certificate, obtaining the certificate through SCEP enrollment, or by importing a certificate in PKCS-12 format. Choose the best option based on the requirements for configuring the CTL file.

**Domain Name**—(Optional) Specifies the domain name of the trustpoint used to create the DNS field for the trustpoint. This is appended to the Common Name field of the Subject DN to create the DNS Name. The domain name should be configured when the FQDN is not configured for the trustpoint. Only one domain-name can be specified.



#### Note

If you are using domain names for your CUCM and TFTP server, you must configure DNS lookup on the security appliance. Add an entry for each of the outside interfaces on the security appliance into your DNS server, if such entries are not already present. Each security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup. Additionally, define your DNS server IP address on the security appliance; for example: `dns name-server 10.2.3.4` (IP address of your DNS server).

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## CTL Provider

Use the CTL Provider option to configure Certificate Trust List provider service.

The CTL Provider pane lets you define and configure Certificate Trust List provider service to enable inspection of encrypted traffic.

#### Fields

- **CTL Provider Name**—Lists the CTL Provider name.
- **Client Details**—Lists the name and IP address of the client.

- Interface Name—Lists the defined interface name.
- IP Address—Lists the defined interface IP address.
- Certificate Name—Lists the certificate to be exported.
- Add—Adds a CTL Provider.
- Edit—Edits a CTL Provider.
- Delete—Deletes a CTL Provider.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit CTL Provider

The Add/Edit CTL Provider dialog box lets you define the parameters for the CTL Provider.

### Fields

- CTL Provider Name—Specifies the CTL Provider name.
- Certificate to be Exported—Specifies the certificate to be exported to the client.
  - Certificate Name—Specifies the name of the certificate to be exported to the client.
  - Manage—Manages identity certificates. See [Identity Certificates Authentication, page 33-6](#)
- Client Details—Specifies the clients allowed to connect.
  - Client to be Added—Specifies the client interface and IP address to add to the client list.
    - Interface—Specifies client interface.
    - IP Address—Specifies the client IP address.
    - Add—Adds the new client to the client list.
    - Delete—Deletes the selected client from the client list.
- More Options—Specifies the available and active algorithms to be announced or matched during the TLS handshake.
  - Parse the CTL file provided by the CTL Client and install trustpoints—Trustpoints installed by this option have names prefixed with “\_internal\_CTL\_.” If disabled, each Call Manager server and CAPF certificate must be manually imported and installed.
  - Port Number—Specifies the port to which the CTL provider listens. The port must be the same as the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default is 2444.
  - Authentication—Specifies the username and password that the client authenticates with the provider.
    - Username—Client username.

Password—Client password.

Confirm Password—Client password.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |





## CHAPTER 20

# Configuring Access Rules and EtherType Rules

This chapter describes how to configure access rules and EtherType rules, and includes the following topics:

- [Information About Access Rules and EtherType Rules, page 20-1](#)
- [Configuring Access Rules, page 20-7](#)
- [Configuring Ethertype Rules \(Transparent Mode Only\), page 20-15](#)



### Note

You use access rules to control network access in both routed and transparent firewall modes. In transparent mode, you can use both access rules (for Layer 3 traffic) and EtherType rules (for Layer 2 traffic).

To access the security appliance interface for management access, you do not also need an access rule allowing the host IP address. You only need to configure management access according to [Chapter 16, “Configuring Management Access.”](#)

## Information About Access Rules and EtherType Rules

Your access policy is made up of one or more access rules and/or EtherType rules per interface.

You can use access rules in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally the source and destination ports.



### Note

To allow any traffic to enter the security appliance, you must attach an inbound access rule to an interface; otherwise, the security appliance automatically drops all traffic that enters that interface.

For transparent mode only, an EtherType rule controls network access for non-IP traffic. An EtherType rule permits or denies traffic based on the EtherType.

This section includes the following topics:

- [Information About Both Access Rules and EtherType Rules, page 20-2](#)
- [Information About Access Rules, page 20-3](#)
- [Information About EtherType Rules, page 20-6](#)

## Information About Both Access Rules and EtherType Rules

This section describes information for both access rules and EtherType rules, and includes the following topics:

- [Using Access Rules and EtherType Rules on the Same Interface, page 20-2](#)
- [Rule Order, page 20-2](#)
- [Implicit Deny, page 20-2](#)
- [Inbound and Outbound Rules, page 20-2](#)

### Using Access Rules and EtherType Rules on the Same Interface

You can apply both access rules and EtherType rules to each direction of an interface.

#### Rule Order

The order of rules is important. When the security appliance decides whether to forward or drop a packet, the security appliance tests the packet against each rule in the order in which the rules are listed. After a match is found, no more rules are checked. For example, if you create an access rule at the beginning that explicitly permits all traffic for an interface, no further rules are ever checked.

You can disable a rule by making it inactive.

#### Implicit Deny

Lists of access rules or EtherType rules have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the security appliance except for particular addresses, then you need to deny the particular addresses and then permit all others.

For EtherType rules, the implicit deny does not affect IPv4 traffic or ARPs; for example, if you allow EtherType 8037 (the EtherType for IPX), the implicit deny at the end of the list does not block any IP traffic that you previously allowed with an access rule (or implicitly allowed from a high security interface to a low security interface). However, if you *explicitly* deny all traffic with an EtherType rule, then IP and ARP traffic is denied.

### Inbound and Outbound Rules

By default, all traffic from a higher-security interface to a lower-security interface is allowed. Access lists let you either allow traffic from lower-security interfaces, or restrict traffic from higher-security interfaces.

The security appliance supports two types of access lists:

- Inbound—Inbound access lists apply to traffic as it enters an interface.
- Outbound—Outbound access lists apply to traffic as it exits an interface.

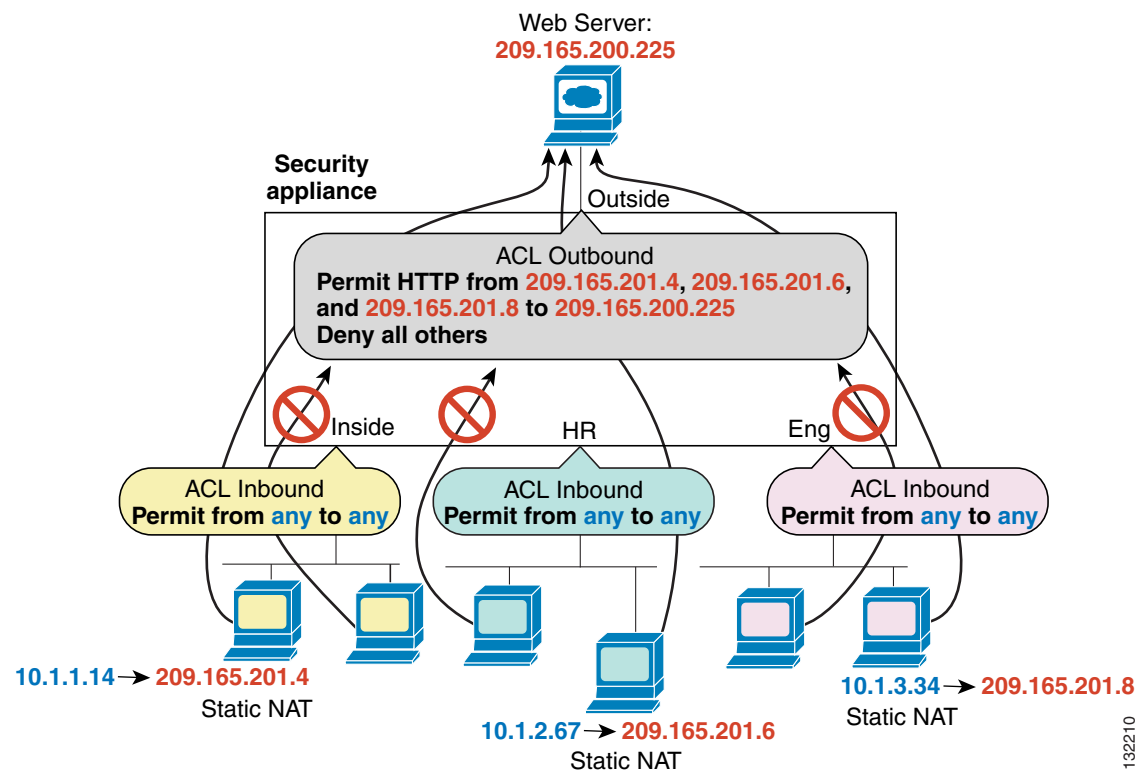


**Note**

“Inbound” and “outbound” refer to the application of an access list on an interface, either to traffic entering the security appliance on an interface or traffic exiting the security appliance on an interface. These terms do not refer to the movement of traffic from a lower security interface to a higher security interface, commonly known as inbound, or from a higher to lower interface, commonly known as outbound.

An outbound access list is useful, for example, if you want to allow only certain hosts on the inside networks to access a web server on the outside network. Rather than creating multiple inbound access lists to restrict access, you can create a single outbound access list that allows only the specified hosts (see Figure 20-1). The outbound access list prevents any other hosts from reaching the outside network.

**Figure 20-1 Outbound Access List**



## Information About Access Rules

This section describes information about access rules, and includes the following topics:

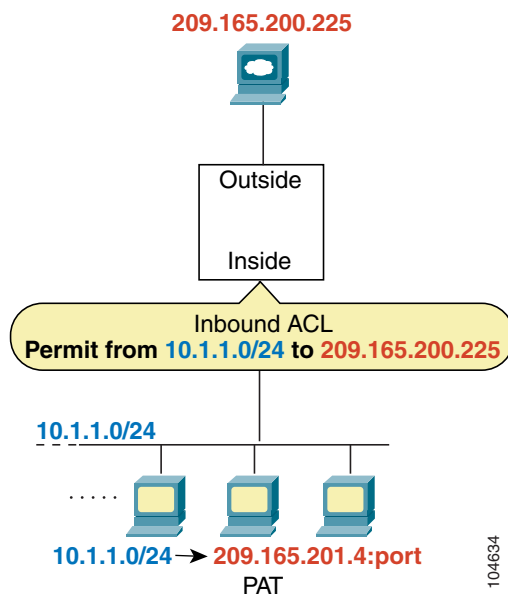
- [IP Addresses Used for Access Rules When You Use NAT, page 20-4](#)
- [Access Rules for Returning Traffic, page 20-6](#)
- [Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules, page 20-6](#)

## IP Addresses Used for Access Rules When You Use NAT

When you use NAT, the IP addresses you specify for an access rule depend on the interface to which the access rule is attached; you need to use addresses that are valid on the network connected to the interface. This guideline applies for both inbound and outbound access rules: the direction does not determine the address used, only the interface does.

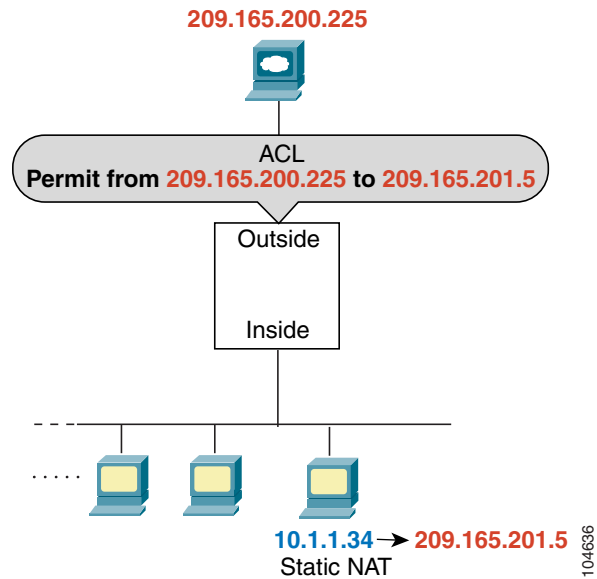
For example, you want to apply an access rule to the inbound direction of the inside interface. You configure the security appliance to perform NAT on the inside source addresses when they access outside addresses. Because the access rule is applied to the inside interface, the source addresses are the original untranslated addresses. Because the outside addresses are not translated, the destination address used in the access rule is the real address (see [Figure 20-2](#)).

**Figure 20-2** IP Addresses in Access Rules: NAT Used for Source Addresses



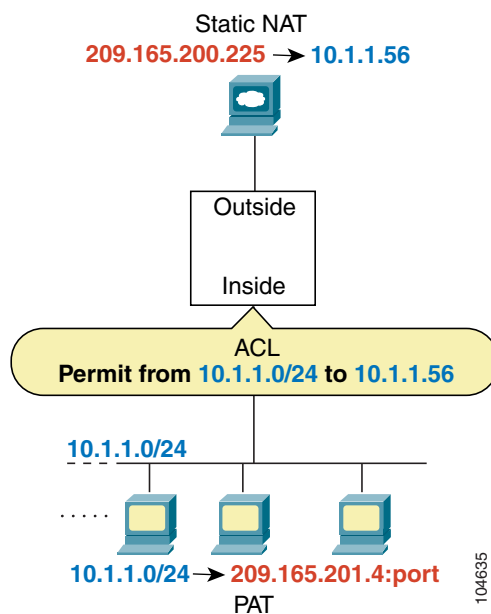
If you want to allow an outside host to access an inside host, you can apply an inbound access rule on the outside interface. You need to specify the translated address of the inside host in the access rule because that address is the address that can be used on the outside network (see [Figure 20-3](#)).

**Figure 20-3** IP Addresses in Access Rules: NAT used for Destination Addresses



If you perform NAT on both interfaces, keep in mind the addresses that are visible to a given interface. In [Figure 20-4](#), an outside server uses static NAT so that a translated address appears on the inside network.

**Figure 20-4** IP Addresses in Access Rules: NAT used for Source and Destination Addresses



## Access Rules for Returning Traffic

For TCP and UDP connections for both routed and transparent mode, you do not need an access list to allow returning traffic, because the security appliance allows all returning traffic for established, bidirectional connections. For connectionless protocols such as ICMP, however, the security appliance establishes unidirectional sessions, so you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections.

## Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules

In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Transparent firewall mode can allow any IP traffic through. This feature is especially useful in multiple context mode, which does not allow dynamic routing, for example.

**Note**

Because these special types of traffic are connectionless, you need to apply an extended access list to both interfaces, so returning traffic is allowed through.

Table 20-1 lists common traffic types that you can allow through the transparent firewall.

**Table 20-1**      *Transparent Firewall Special Traffic*

| Traffic Type      | Protocol or Port                                 | Notes                                                                                  |
|-------------------|--------------------------------------------------|----------------------------------------------------------------------------------------|
| DHCP              | UDP ports 67 and 68                              | If you enable the DHCP server, then the security appliance does not pass DHCP packets. |
| EIGRP             | Protocol 88                                      | —                                                                                      |
| OSPF              | Protocol 89                                      | —                                                                                      |
| Multicast streams | The UDP ports vary depending on the application. | Multicast streams are always destined to a Class D address (224.0.0.0 to 239.x.x.x).   |
| RIP (v1 or v2)    | UDP port 520                                     | —                                                                                      |

## Information About EtherType Rules

This section describes EtherType rules, and includes the following topics:

- [Supported EtherTypes, page 20-6](#)
- [Implicit Permit of IP and ARPs Only, page 20-7](#)
- [Using Access Rules and EtherType Rules on the Same Interface, page 20-2](#)
- [Allowing MPLS, page 20-7](#)

## Supported EtherTypes

An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number.

EtherType rules support Ethernet V2 frames.

802.3-formatted frames are not handled by the rule because they use a length field as opposed to a type field.

BPDUs, which are handled by the rule, are the only exception: they are SNAP-encapsulated, and the security appliance is designed to specifically handle BPDUs.

The security appliance receives trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the security appliance modifies the payload with the outgoing VLAN if you allow BPDUs.

**Note**

If you use failover, you must allow BPDUs on both interfaces with an EtherType rule to avoid bridging loops.

## Implicit Permit of IP and ARPs Only

IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without a rule. ARPs are allowed through the transparent firewall in both directions without a rule. ARP traffic can be controlled by ARP inspection.

However, to allow any traffic with EtherTypes other than IPv4 and ARP, you need to apply an EtherType access list, even from a high security to a low security interface.

Because EtherTypes are connectionless, you need to apply the rule to both interfaces if you want traffic to pass in both directions.

## IPv6 Unsupported

EtherType ACEs do not allow IPv6 traffic, even if you specify the IPv6 EtherType.

## Allowing MPLS

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the security appliance by configuring both MPLS routers connected to the security appliance to use the IP address on the security appliance interface as the router-id for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

On Cisco IOS routers, enter the appropriate command for your protocol, LDP or TDP. The *interface* is the interface connected to the security appliance.

```
hostname(config)# mpls ldp router-id interface force
```

Or

```
hostname(config)# tag-switching tdp router-id interface force
```

# Configuring Access Rules

The Access Rules window shows your entire network security policy expressed in rules.

When you choose the **Access Rules** option, this window lets you define access lists to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

For more information about access rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

### Fields

Note: You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

- Add—Adds a new access rule.
- Edit—Edits an access rule.
- Delete—Deletes an access rule.
- Move Up—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- Move Down—Moves a rule down.
- Cut—Cuts a rule.
- Copy—Copies the parameters of a rule so you can start a new rule with the same parameters using the Paste button.
- Paste—Opens an Add/Edit Rule dialog box with the copied or cut parameters of a rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.
- Find—Filters the display to show only matching rules. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
  - Filter drop-down list—Choose the criteria to filter on, either Interface, Source, Destination, Source or Destination, Destination Service, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
  - Condition drop-down list—For criteria Source, Destination, Source or Destination, and Destination Service, choose the condition, either is or includes.
  - Filter field—For the Interface type, this field becomes a drop-down list so you can choose an interface name. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually, or browse for one by clicking the ... button and launching the Browse Address dialog box. The Destination Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the ... button and launching the Browse Service Groups dialog box. The Filter field accepts multiple entries separated by a comma or space. Wildcards are also allowed.
  - Filter—Runs the filter.
  - Clear—Clears the matches and displays all.
  - Rule Query—Opens the Rule Queries dialog box so you can manage named rule queries.
- Diagram—Shows the Rule Flow Diagram area under the rule table. This diagram shows the networks, type of traffic, interface name, direction of flow, and action.
- Export—Exports to a file in either comma separated value or html format.
- Show—Shows the syslogs generated by the selected access rule in the Real-Time Log Viewer.

The following description summarizes the columns in the Access Rules table. You can edit the contents of these columns by double-clicking on a table row. Rules are displayed in the order of execution. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- **No**—Indicates the order of evaluation for the rule.
- **Enabled**—Indicates whether the rule is enabled or disabled.
- **Source**—Specifies the IP address, network object group, interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination Type field. An address column might contain an interface name with the word any, such as inside:any. This means that any host on the inside interface is affected by the rule.
- **Destination**—Specifies the IP address, network object group, interface IP, or any, to which traffic is permitted or denied from the source specified in the Source Type field. An address column might contain an interface name with the word any, such as outside:any. This 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 firewall maps the address of the inside host to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. The address mapping structure is called an xlate, and remains in memory for a period of time. During this time, outside hosts can initiate connections to the inside host using the translated address from the pool, if allowed by the access rule. Normally, outside-to-inside connections require a static translation so that the inside host always uses the same IP address.
- **Service**—Shows the service or protocol specified by the rule.
- **Action**—The action that applies to the rule, either Permit or Deny.
- **Hits**—Shows the number of hits for the rule. This column is dynamically updated depending on the frequency set in the Preferences dialog box. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
- **Logging**—If you enable logging for the access rule, this column shows the logging level and the interval in seconds between log messages.
- **Time**—Displays the time range during which the rule is applied.
- **Description**—Shows the description you entered when you added the rule. An implicit rule includes the following description: “Implicit outbound rule.”
- **Addresses**—Tab that lets you add, edit, delete, or find IP names or network object groups. IP address objects are automatically created based on source and destination entries during rule creation so that they can easily be selected in the creation of subsequent rules. They cannot be added, edited, or deleted manually.
- **Services**—Tab that lets you add, edit, delete, or find services.
- **Time Ranges**—Tab that lets you add, edit, or delete time ranges.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Rule Queries

The Rule Queries dialog box lets you manage named rule queries that you can use in the Filter field when searching for Rules.

### Fields

- Add—Adds a rule query.
- Edit—Edits a rule query.
- Delete—Deletes a rule query.
- Name—Lists the names of the rule queries.
- Description—Lists the descriptions of the rule queries.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## New/Edit Rule Query

The New/Edit Rule Query dialog box lets you add or edit a named rule query that you can use in the Filter field when searching for Rules.

### Fields

- Name—Enter a name for this rule query.
- Description—Enter a description for this rule query.
- Match Criteria—This area lists the criteria you want to filter on.
  - any of the following criteria—Sets the rule query to match any of the listed criteria.
  - all of the following criteria—Sets the rule query to match all of the listed criteria.
  - Field—Lists the type of criteria. For example, an interface or source.
  - Value—Lists the value of the criteria, for example, “inside.”
  - Remove—Removes the selected criteria.
- Define New Criteria—This area lets you define new criteria to add to the match criteria.



- Field—Choose a type of criteria, including Interface, Source, Destination, Service, Action, or another Rule Query to be nested in this rule query.
- Value—Enter a value to search on. For the Interface type, this field becomes a drop-down list so you can choose an interface name. For the Action type, the drop-down list includes Permit and Deny. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually, or browse for one by clicking the ... button and launching the Browse Address dialog box. The Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the ... button and launching the Browse Service Groups dialog box.
- Add—Adds the criteria to the Match Criteria table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Access Rule

The Add/Edit Rule dialog box lets you create a new rule, or modify an existing rule.

For more information about access rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

### Fields

- Interface—Specifies the interface to which the rule applies.
- Action—Determines the action type of the new rule. Select either permit or deny.
  - Permit—Permits all matching traffic.
  - Deny—Denies all matching traffic.
- Source—Specifies the IP address, network object group, interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination field.
  - ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- Destination —Specifies the IP address, network object group, interface IP, or any, to which traffic is permitted or denied from the source specified in the Source Type field.
  - ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- Service—Choose this option to specify a port number, a range of ports, or a well-known service name or group from a list of services.
  - ...—Lets you select, add, edit, delete, or find an existing service from a preconfigured list.
- Description—(Optional) Enter a description of the access rule.
- Enable Logging—Enables logging for the access rule.

- Logging Level—Specifies default, emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
- More Options—Shows additional configuration options for the rule.
  - Enable Rule—Enables or disables the rule.
  - Traffic Direction—Determines which direction of traffic the rule is applied. Options are either incoming or outgoing.
  - Source Service—Specifies a source protocol and service (TCP or UDP service only).
    - ...—Lets you select, add, edit, delete or find a source service from a preconfigured list.
  - Logging Interval—Specifies the interval for logging in seconds if logging is configured.
  - Time Range—Specifies a time range defined for this rule from the drop-down list.
    - ...—Lets you select, add, edit, delete or find a time range from a preconfigured list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Manage Service Groups

The Manage Service Groups dialog box lets you associate multiple TCP, UDP, or TCP-UDP services (ports) in a named group. You can then use the service group in an access or IPSec rule, a conduit, or other functions within ASDM and the CLI.

The term service refers to higher layer protocols associated with application level services having well known port numbers and “literal” names such as ftp, telnet, and smtp.

The security appliance permits the following TCP literal names:

bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, www.

The Name of a service group must be unique to all four types of object groups. For example, a service group and a network group may not share the same name.

Multiple service groups can be nested into a “group of groups” and used the same as a single group. When a service object group is deleted, it is removed from all service object groups where it is used.

If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

### Fields

- TCP—Select this option to add TCP services or port numbers to an object group.
- UDP—Select this option to add UDP services or port numbers to an object group.

- **TCP-UDP**—Select this option to add services or port numbers that are common to TCP and UDP to an object group.
- **Service Group table**—This table contains a descriptive name for each service object group. To modify or delete a group on this list, select the group and click **Edit** or **Delete**. To add a new group to this list, click **Add**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Service Group

The Add/Edit Service Group dialog box lets you manage a group of TCP/UDP services/ports.

### Fields

- **Service Group Name**—Specifies the name of the service group. The name must be unique for all object groups. A service group name cannot share a name with a network group.
- **Description**—Specifies a description of the service group.
- **Service**—Lets you select services for the service group from a predefined drop-down list.
- **Range/Port #**—Lets you specify a range of ports for the service group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Advanced Access Rule Configuration

The Advanced Access Rule Configuration dialog box lets you to set global access rule logging options.

When you enable logging, if a packet matches the access rule, the security appliance creates a flow entry to track the number of packets received within a specific interval (see Log Options). The security appliance generates a system log message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the security appliance resets the hit count to 0. If no packets match the access rule during an interval, the security appliance deletes the flow entry.

A large number of flows can exist concurrently at any point of time. To prevent unlimited consumption of memory and CPU resources, the security appliance places a limit on the number of concurrent deny flows; the limit is placed only on deny flows (and not permit flows) because they can indicate an attack. When the limit is reached, the security appliance does not create a new deny flow until the existing flows expire. If someone initiates a denial of service attack, the security appliance can create a very large number of deny flows in a very short period of time. Restricting the number of deny-flows prevents unlimited consumption of memory and CPU resources.

For more information about access rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

**Prerequisites**

These settings only apply if you enable the newer logging mechanism for the access control entry (also known as a rule) for the access rule. See Log Options for more information.

**Fields**

- **Maximum Deny-flows**—The maximum number of deny flows permitted before the security appliance stops logging, between 1 and the default value. The default is 4096.
- **Alert Interval**—The amount of time (1-3600 seconds) between system log messages (number 106101) that identify that the maximum number of deny flows was reached. The default is 300 seconds.
- **Per User Override table**—Specifies the state of the per user override feature. If the per user override feature is enabled on the inbound access rule, the access rule provided by a RADIUS server replaces the access rule configured on that interface. If the per user override feature is disabled, the access rule provided by the RADIUS server is combined with the access rule configured on that interface. If the inbound access rule is not configured for the interface, per user override cannot be configured.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# Log Options

The Log Options dialog box lets you set logging options for each access rule. See the [“Advanced Access Rule Configuration” section on page 20-13](#) to set global logging options.

This dialog box lets you use the older logging mechanism (only denied traffic is logged), to use the newer logging mechanism (permitted and denied traffic is logged, along with additional information such as how many packet hits), or to disable logging.

The Log option consumes a certain amount of memory when enabled. To help control the risk of a potential Denial of Service attack, you can configure the Maximum Deny-flow setting by choosing **Advanced** in the Access Rules window.

**Fields**

- Use default logging behavior—Uses the older access rule logging mechanism: the security appliance logs system log message number 106023 when a packet is denied. Use this option to return to the default setting.
- Enable logging for the rule—Enables the newer access rule logging mechanism: the security appliance logs system log message number 106100 when a packet matches the access rule (either permit or deny).

If a packet matches the access rule, the security appliance creates a flow entry to track the number of packets received within a specific interval (see the Logging Interval field that follows). The security appliance generates a system log message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the security appliance resets the hit count to 0. If no packets match the access rule during an interval, the security appliance deletes the flow entry.

- Logging Level—Selects the level of logging messages to be sent to the syslog server from this drop-down list. Levels are defined as follows:

Emergency (level 0)—The security appliance does not use this level.

Alert (level 1, immediate action needed)

Critical (level 2, critical condition)

Error (level 3, error condition)

Warning (level 4, warning condition)

Notification (level 5, normal but significant condition)

Informational (level 6, informational message only)

Debugging (level 7, appears during debugging only)

- Logging Interval—Sets the amount of time in seconds (1-600) the security appliance waits before sending the flow statistics to the syslog. This setting also serves as the timeout value for deleting a flow if no packets match the access rule. The default is 300 seconds.

- Disable logging for the rule—Disables all logging for the access rule.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring EtherType Rules (Transparent Mode Only)

The EtherType Rules window shows access rules based on packet EtherTypes. EtherType rules are used to configure non-IP related traffic policies through the security appliance when operating in transparent mode. In transparent mode, you can apply both extended and EtherType access rules to an interface. EtherType rules take precedence over the extended access rules.

For more information about EtherType rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

### Fields

- **Add**—Adds a new EtherType rule. Choose the type of rule you want to add from the drop-down list.
- **Edit**—Edits an EtherType rule.
- **Delete**—Deletes an EtherType rule.
- **Move Up**—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- **Move Down**—Moves a rule down.
- **Cut**—Cuts a rule.
- **Copy**—Copies the parameters of a rule so you can start a new rule with the same parameters using the Paste button.
- **Paste**—Opens an Add/Edit Rule dialog box with the copied or cut parameters of the rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.

The following description summarizes the columns in the EtherType Rules table. You can edit the contents of these columns by double-clicking on a table cell. Double-clicking on a column header sorts the table in ascending alphanumeric order, using the selected column as the sort key. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- **No**—Indicates the order of evaluation for the rule.
- **Action**—Permit or deny action for this rule.
- **Ethertype**—EtherType value: IPX, BPDU, MPLS-Unicast, MPLS-Multicast, or a 16-bit hexadecimal value between 0x600 (1536) and 0xffff by which an EtherType can be identified.
- **Interface**—Interface to which the rule is applied.
- **Direction Applied**—Direction for this rule: incoming traffic or outgoing traffic.
- **Description**—Optional text description of the rule.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |

## Add/Edit EtherType Rule

The Add/Edit EtherType Rules dialog box lets you add or edit an EtherType rule.

For more information about EtherType rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

### Fields

- Action—Permit or deny action for this rule.
- Interface—Interface name for this rule.
- Apply rule to—Direction for this rule: incoming traffic or outgoing traffic.
- Ethertype—EtherType value: BPDU, IPX, MPLS-Unicast, MPLS-Multicast, any (any value between 0x600 and 0xffff), or a 16-bit hexadecimal value between 0x600 (1536) and 0xffff by which an EtherType can be identified.
- Description—Optional text description of the rule.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |







# CHAPTER 21

## Configuring NAT

---

This chapter describes Network Address Translation, and includes the following sections:

- [NAT Overview, page 21-1](#)
- [Configuring NAT Control, page 21-15](#)
- [Using Dynamic NAT, page 21-16](#)
- [Using Static NAT, page 21-25](#)
- [Using NAT Exemption, page 21-30](#)

## NAT Overview

This section describes how NAT works on the security appliance, and includes the following topics:

- [Introduction to NAT, page 21-1](#)
- [NAT Control, page 21-4](#)
- [NAT Types, page 21-6](#)
- [Policy NAT, page 21-10](#)
- [NAT and Same Security Level Interfaces, page 21-12](#)
- [Order of NAT Rules Used to Match Real Addresses, page 21-13](#)
- [Mapped Address Guidelines, page 21-13](#)
- [DNS and NAT, page 21-13](#)

## Introduction to NAT

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is composed of two steps: the process by which a real address is translated into a mapped address, and the process to undo translation for returning traffic.

The security appliance translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet continues. The exception is when you enable NAT control. NAT control requires that packets traversing from a higher security interface (inside) to a lower security interface (outside) match a NAT rule, or processing for the packet stops. See the [“Default Security Level” section on page 7-4](#) for more information about security levels. See the [“NAT Control” section on page 21-4](#) for more information about NAT control.

**Note**

In this document, all types of translation are referred to as NAT. When describing NAT, the terms *inside* and *outside* represent the security relationship between any two interfaces. The higher security level is inside and the lower security level is outside. For example, interface 1 is at 60 and interface 2 is at 50; therefore, interface 1 is “inside” and interface 2 is “outside.”

Some of the benefits of NAT are as follows:

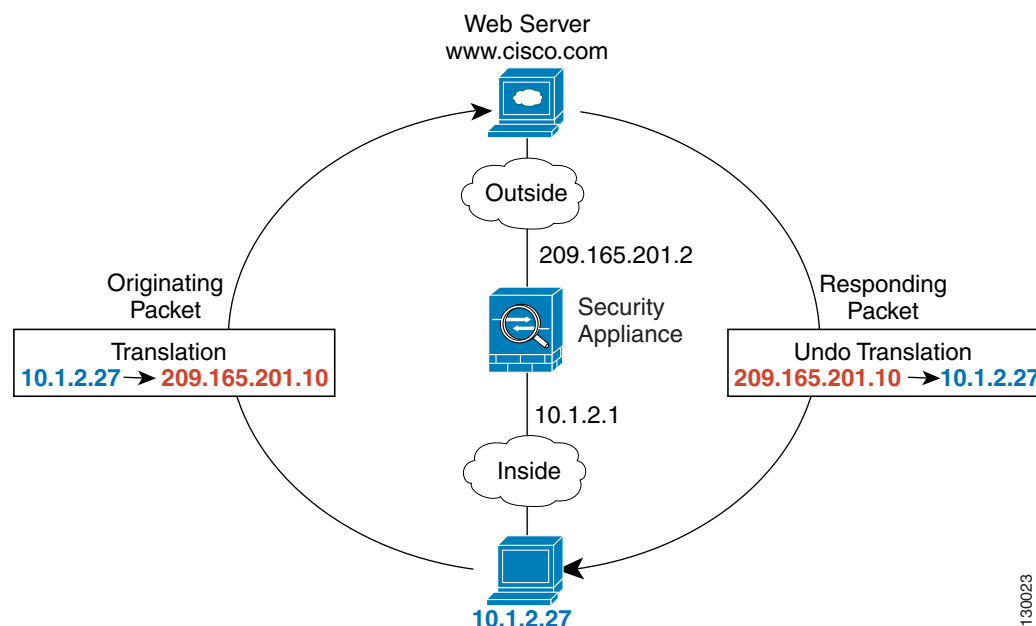
- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the real addresses from other networks, so attackers cannot learn the real address of a host.
- You can resolve IP routing problems such as overlapping addresses.

See [Table 24-1 on page 24-3](#) for information about protocols that do not support NAT.

## NAT in Routed Mode

Figure 21-1 shows a typical NAT example in routed mode, with a private network on the inside. When the inside host at 10.1.1.27 sends a packet to a web server, the real source address, 10.1.1.27, of the packet is changed to a mapped address, 209.165.201.10. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the security appliance receives the packet. The security appliance then changes the translation of the mapped address, 209.165.201.10 back to the real address, 10.1.1.27 before sending it to the host.

**Figure 21-1 NAT Example: Routed Mode**



130023

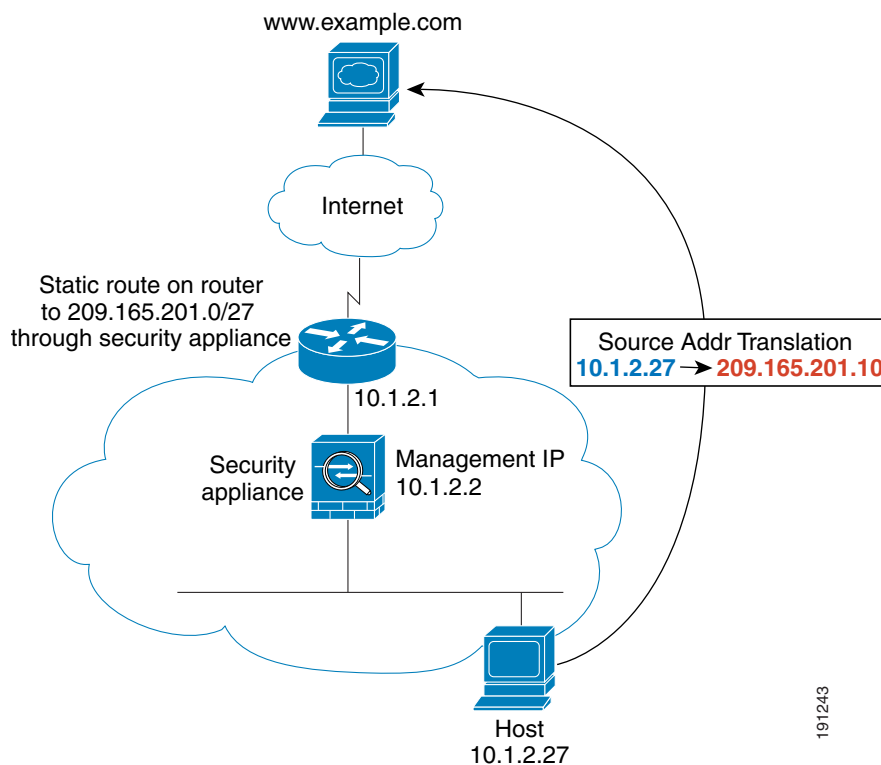
## NAT in Transparent Mode

Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks. For example, a transparent firewall security appliance is useful between two VRFs so you can establish BGP neighbor relations between the VRFs and the global table. However, NAT per VRF might not be supported. In this case, using NAT in transparent mode is essential.

NAT in transparent mode has the following requirements and limitations:

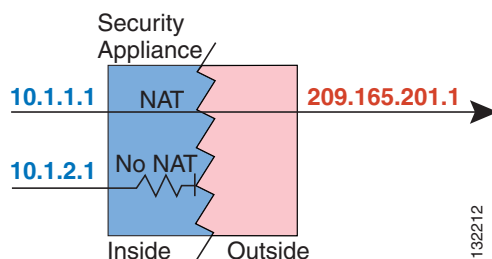
- When the mapped addresses are not on the same network as the transparent firewall, then on the upstream router, you need to add a static route for the mapped addresses that points to the downstream router (through the security appliance).
- If the real destination address is not directly-connected to the security appliance, then you also need to add a static route on the security appliance for the real destination address that points to the downstream router. Without NAT, traffic from the upstream router to the downstream router does not need any routes on the security appliance because it uses the MAC address table. NAT, however, causes the security appliance to use a route lookup instead of a MAC address lookup, so it needs a static route to the downstream router.
- The **alias** command is not supported.
- Because the transparent firewall does not have any interface IP addresses, you cannot use interface PAT.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the firewall sends an ARP request to a host on the other side of the firewall, and the initiating host real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.

Figure 21-2 shows a typical NAT scenario in transparent mode, with the same network on the inside and outside interfaces. The transparent firewall in this scenario is performing the NAT service so that the upstream router does not have to perform NAT. When the inside host at 10.1.1.27 sends a packet to a web server, the real source address of the packet, 10.1.1.27, is changed to a mapped address, 209.165.201.10. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the security appliance receives the packet because the upstream router includes this mapped network in a static route directed through the security appliance. The security appliance then undoes the translation of the mapped address, 209.165.201.10 back to the real address, 10.1.1.1.27. Because the real address is directly-connected, the security appliance sends it directly to the host.

**Figure 21-2 NAT Example: Transparent Mode**

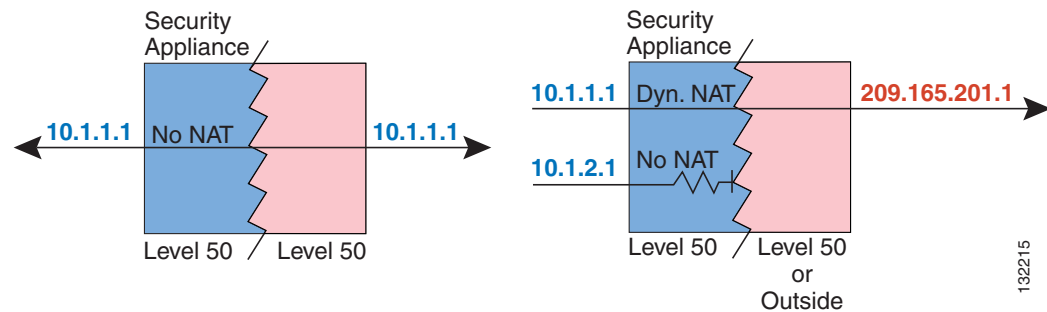
## NAT Control

NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule; for any host on the inside network to access a host on the outside network, you must configure NAT to translate the inside host address, as shown in [Figure 21-3](#).

**Figure 21-3 NAT Control and Outbound Traffic**

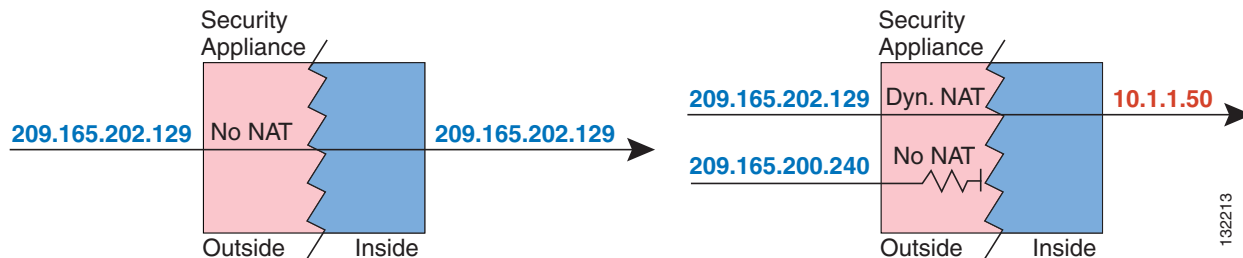
Interfaces at the same security level are not required to use NAT to communicate. However, if you configure dynamic NAT or PAT on a same security interface, then all traffic from the interface to a same security interface or an outside interface must match a NAT rule, as shown in [Figure 21-4](#).

**Figure 21-4 NAT Control and Same Security Traffic**



Similarly, if you enable outside dynamic NAT or PAT, then all outside traffic must match a NAT rule when it accesses an inside interface (see [Figure 21-5](#)).

**Figure 21-5 NAT Control and Inbound Traffic**



Static NAT does not cause these restrictions.

By default, NAT control is disabled; therefore, you do not need to perform NAT on any networks unless you want to do so. If you upgraded from an earlier version of software, however, NAT control might be enabled on your system. Even with NAT control disabled, you need to perform NAT on any addresses for which you configure dynamic NAT. See the [“Dynamic NAT Implementation”](#) section on page 21-16 for more information about how dynamic NAT is applied.

If you want the added security of NAT control but do not want to translate inside addresses in some cases, you can apply a NAT exemption or identity NAT rule on those addresses. (See the [“Using NAT Exemption”](#) section on page 21-30 for more information).

To configure NAT control, see the [“Configuring NAT Control”](#) section on page 21-15.



**Note**

In multiple context mode, the packet classifier might rely on the NAT configuration to assign packets to contexts if you do not enable unique MAC addresses for shared interfaces. See the [“How the Security Appliance Classifies Packets”](#) section on page 10-2 for more information about the relationship between the classifier and NAT.

## NAT Types

This section describes the available NAT types, and includes the following topics:

- [Dynamic NAT, page 21-6](#)
- [PAT, page 21-8](#)
- [Static NAT, page 21-8](#)
- [Static PAT, page 21-9](#)
- [Bypassing NAT When NAT Control is Enabled, page 21-10](#)

You can implement address translation as dynamic NAT, Port Address Translation, static NAT, static PAT, or as a mix of these types. You can also configure rules to bypass NAT; for example, to enable NAT control when you do not want to perform NAT.

### Dynamic NAT

Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool may include fewer addresses than the real group. When a host you want to translate accesses the destination network, the security appliance assigns the host an IP address from the mapped pool. The translation is added only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, although the connection is allowed by an access list, and the security appliance rejects any attempt to connect to a real host address directly. See the “[Static NAT](#)” or “[Static PAT](#)” section for information on how to obtain reliable access to hosts.

**Note**

---

In some cases, a translation is added for a connection, although the session is denied by the security appliance. This condition occurs with an outbound access list, a management-only interface, or a backup interface in which the translation times out normally.

---

[Figure 21-6](#) shows a remote host attempting to connect to the real address. The connection is denied, because the security appliance only allows returning connections to the mapped address.

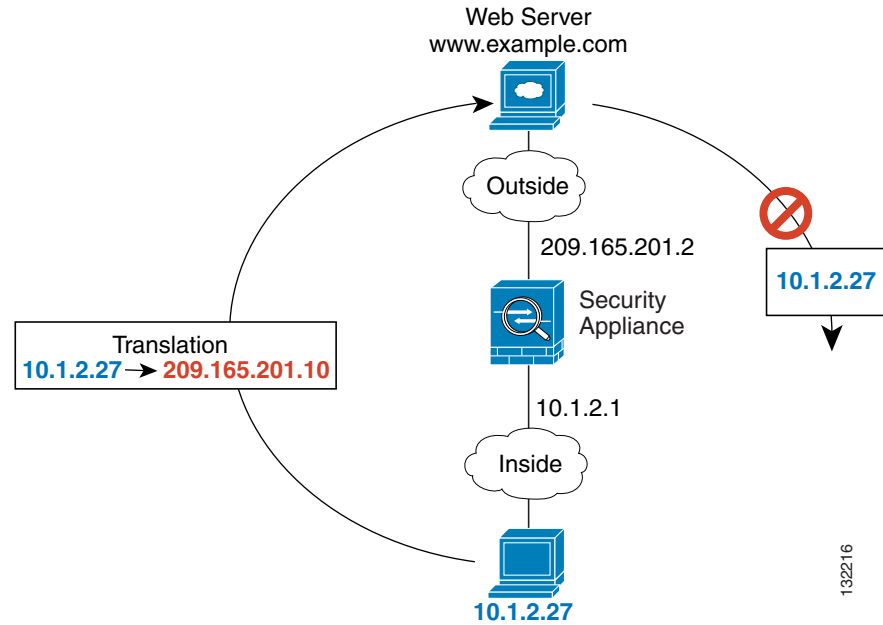
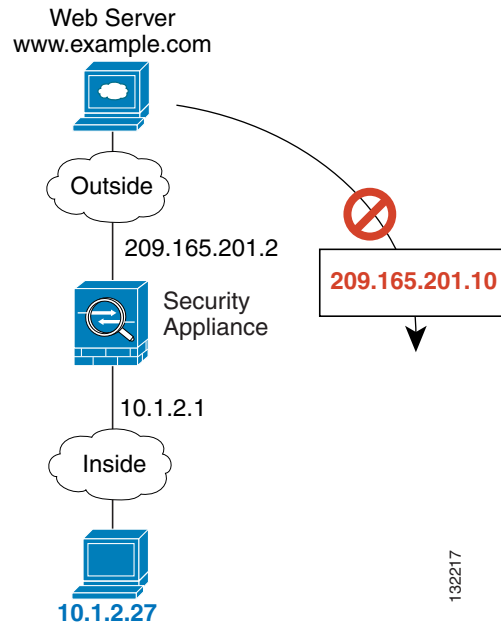
**Figure 21-6 Remote Host Attempts to Connect to the Real Address**

Figure 21-7 shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the security appliance drops the packet.

**Figure 21-7 Remote Host Attempts to Initiate a Connection to a Mapped Address****Note**

For the duration of the translation, a remote host can initiate a connection to the translated host if an access list allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case, you can rely on the security of the access list.

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

Use PAT if this event occurs often, because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool; if the destination network requires registered addresses, such as the Internet, you might encounter a shortage of usable addresses.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.
- Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

See the [“When to Use Application Protocol Inspection” section on page 24-2](#) for more information about NAT and PAT support.

## PAT

PAT translates multiple real addresses to a single mapped IP address. Specifically, the security appliance translates the real address and source port (real socket) to the mapped address and a unique port above 1024 (mapped socket). Each connection requires a separate translation, because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

After the connection expires, the port translation also expires after 30 seconds of inactivity. The timeout is not configurable. Users on the destination network cannot reliably initiate a connection to a host that uses PAT (even if the connection is allowed by an access list). Not only can you not predict the real or mapped port number of the host, but the security appliance does not create a translation at all unless the translated host is the initiator. See the following [“Static NAT”](#) or [“Static PAT”](#) sections for reliable access to hosts.

PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the security appliance interface IP address as the PAT address. PAT does not work with some multimedia applications that have a data stream that is different from the control path. See the [“When to Use Application Protocol Inspection” section on page 24-2](#) for more information about NAT and PAT support.



### Note

For the duration of the translation, a remote host can initiate a connection to the translated host if an access list allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case, you can rely on the security of the access list. However, policy PAT does not support time-based ACLs.

## Static NAT

Static NAT creates a fixed translation of real address(es) to mapped address(es). With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if an access list exists that allows it).



The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if an access list exists that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

## Static PAT

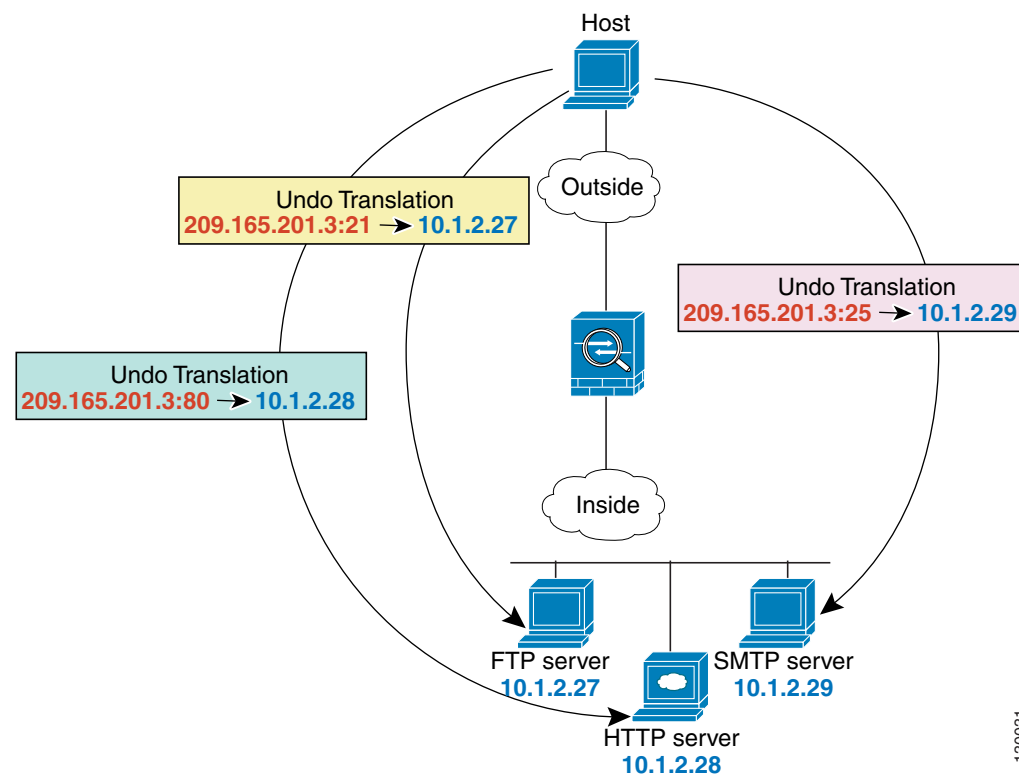
Static PAT is the same as static NAT, except that it lets you specify the protocol (TCP or UDP) and port for the real and mapped addresses.

This feature lets you identify the same mapped address across many different static statements, provided the port is different for each statement. You cannot use the same mapped address for multiple static NAT statements.

For applications that require inspection for secondary channels (for example, FTP and VoIP), the security appliance automatically translates the secondary ports.

For example, if you want to provide a single address for remote users to access FTP, HTTP, and SMTP, but these are all actually different servers on the real network, you can specify static PAT statements for each server that uses the same mapped IP address, but different ports (see [Figure 21-8](#)).

**Figure 21-8**      **Static PAT**



You can also use static PAT to translate a well-known port to a non-standard port or vice versa. For example, if inside web servers use port 8080, you can allow outside users to connect to port 80, and then undo translation to the original port 8080. Similarly, to provide extra security, you can tell web users to connect to non-standard port 6785, and then undo translation to port 80.

## Bypassing NAT When NAT Control is Enabled

If you enable NAT control, then inside hosts must match a NAT rule when accessing outside hosts. If you do not want to perform NAT for some hosts, then you can bypass NAT for those hosts or you can disable NAT control. You might want to bypass NAT, for example, if you are using an application that does not support NAT. See the [“When to Use Application Protocol Inspection” section on page 24-2](#) for information about inspection engines that do not support NAT.

You can configure traffic to bypass NAT using one of three methods. All methods achieve compatibility with inspection engines. However, each method offers slightly different capabilities, as follows:

- **Identity NAT**—When you configure identity NAT (which is similar to dynamic NAT), you do not limit translation for a host on specific interfaces; you must use identity NAT for connections through all interfaces. Therefore, you cannot choose to perform normal translation on real addresses when you access interface A, but use identity NAT when accessing interface B. Regular dynamic NAT, on the other hand, lets you specify a particular interface on which to translate the addresses. Make sure that the real addresses for which you use identity NAT are routable on all networks that are available according to your access lists.

For identity NAT, even though the mapped address is the same as the real address, you cannot initiate a connection from the outside to the inside (even if the interface access list allows it). Use static identity NAT or NAT exemption for this functionality.

- **Static identity NAT**—Static identity NAT lets you specify the interface on which you want to allow the real addresses to appear, so you can use identity NAT when you access interface A, and use regular translation when you access interface B. Static identity NAT also lets you use policy NAT, which identifies the real and destination addresses when determining the real addresses to translate (see the [“Policy NAT” section on page 21-10](#) for more information about policy NAT). For example, you can use static identity NAT for an inside address when it accesses the outside interface and the destination is server A, but use a normal translation when accessing the outside server B.
- **NAT exemption**—NAT exemption allows both translated and remote hosts to initiate connections. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption does let you specify the real and destination addresses when determining the real addresses to translate (similar to policy NAT), so you have greater control using NAT exemption. However unlike policy NAT, NAT exemption does not consider the ports in the access list. NAT exemption also does not let you configure connection limits such as maximum TCP connections.

## Policy NAT

Policy NAT lets you identify real addresses for address translation by specifying the source and destination addresses. You can also optionally specify the source and destination ports. Regular NAT can only consider the source addresses, and not the destination. For example, with policy NAT, you can translate the real address to mapped address A when it accesses server A, but translate the real address to mapped address B when it accesses server B.

For applications that require application inspection for secondary channels (for example, FTP and VoIP), the policy specified in the policy NAT rule should include the secondary ports. When the ports cannot be predicted, the policy should specify only the IP addresses for the secondary channel. With this configuration, the security appliance translates the secondary ports.

[Figure 21-9](#) shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129. When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130. Consequently, the host appears to be on the same network as the servers, which can help with routing.

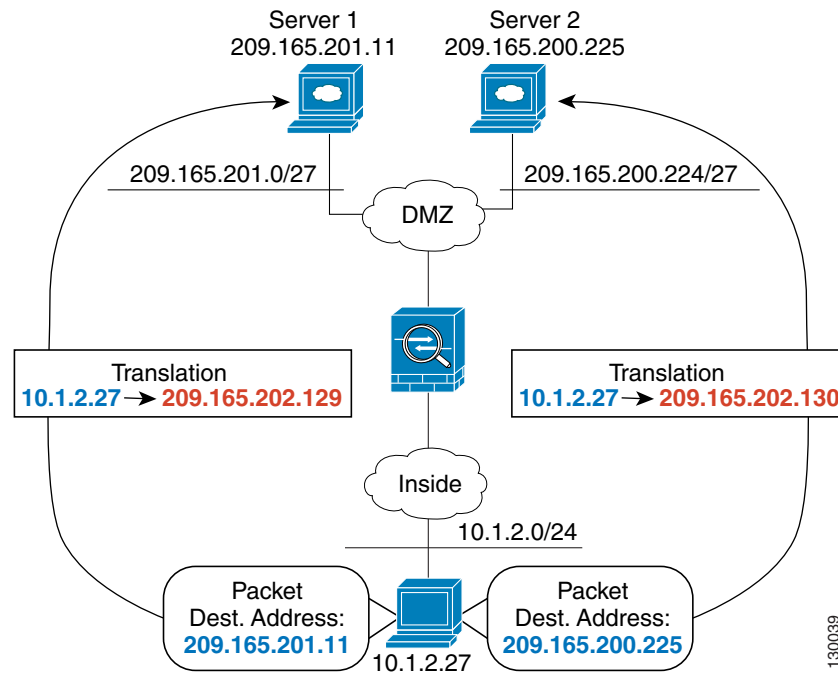
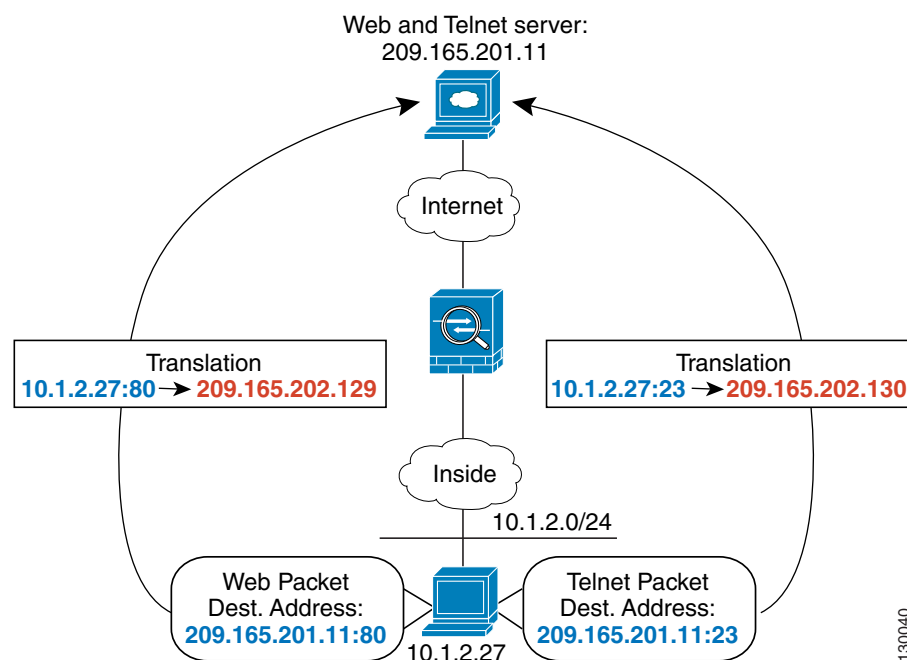
**Figure 21-9 Policy NAT with Different Destination Addresses**

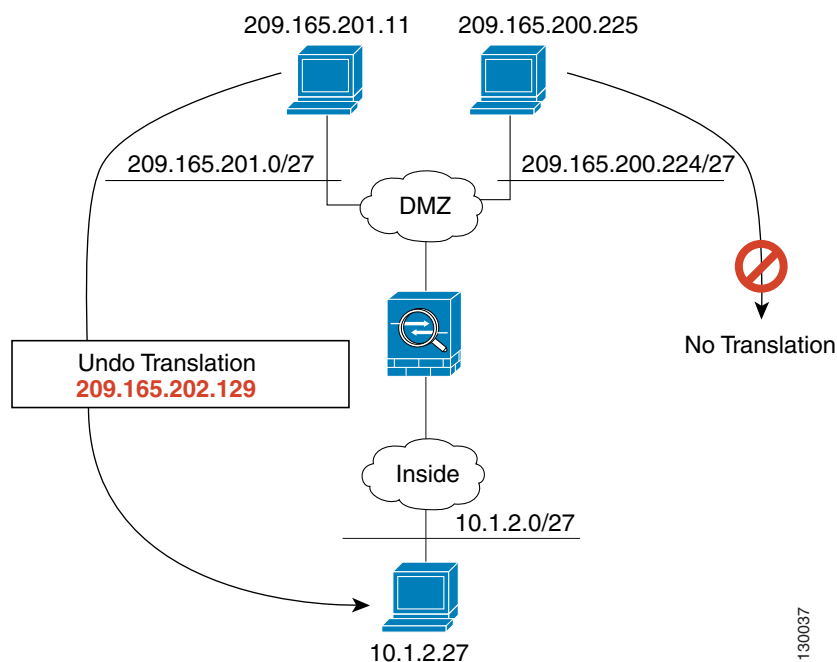
Figure 21-10 shows the use of source and destination ports. The host on the 10.1.2.0/24 network accesses a single host for both web services and Telnet services. When the host accesses the server for web services, the real address is translated to 209.165.202.129. When the host accesses the same server for Telnet services, the real address is translated to 209.165.202.130.

**Figure 21-10 Policy NAT with Different Destination Ports**

For policy static NAT, both translated and remote hosts can originate traffic. For traffic originated on the translated network, the NAT rule specifies the real addresses and the *destination* addresses, but for traffic originated on the remote network, the rule identifies the real addresses and the *source* addresses of remote hosts who are allowed to connect to the host using this translation.

Figure 21-11 shows a remote host connecting to a translated host. The translated host has a policy static NAT translation that translates the real address only for traffic to and from the 209.165.201.0/27 network. A translation does not exist for the 209.165.200.224/27 network, so the translated host cannot connect to that network, nor can a host on that network connect to the translated host.

**Figure 21-11 Policy Static NAT with Destination Address Translation**



**Note**

Policy NAT does not support SQL\*Net, but it is supported by regular NAT. See the [“When to Use Application Protocol Inspection”](#) section on page 24-2 for information about NAT support for other protocols.

## NAT and Same Security Level Interfaces

NAT is not required between same security level interfaces even if you enable NAT control. You can optionally configure NAT if desired. However, if you configure dynamic NAT when NAT control is enabled, then NAT is required. See the [“NAT Control”](#) section on page 21-4 for more information. Also, when you specify a group of IP address(es) for dynamic NAT or PAT on a same security interface, then you must perform NAT on that group of addresses when they access any lower or same security level interface (even when NAT control is not enabled). Traffic identified for static NAT is not affected.



**Note**

The security appliance does not support VoIP inspection engines when you configure NAT on same security interfaces. These inspection engines include Skinny, SIP, and H.323. See the [“When to Use Application Protocol Inspection”](#) section on page 24-2 for supported inspection engines.

## Order of NAT Rules Used to Match Real Addresses

The security appliance matches real addresses to NAT rules in the following order:

1. NAT exemption—In order, until the first match.
2. Static NAT and Static PAT (regular and policy)—In order, until the first match. Static identity NAT is included in this category.
3. Policy dynamic NAT—In order, until the first match. Overlapping addresses are allowed.
4. Regular dynamic NAT—Best match. Regular identity NAT is included in this category. The order of the NAT rules does not matter; the NAT rule that best matches the real address is used. For example, you can create a general rule to translate all addresses (0.0.0.0) on an interface. If you want to translate a subset of your network (10.1.1.1) to a different address, then you can create a rule to translate only 10.1.1.1. When 10.1.1.1 makes a connection, the specific rule for 10.1.1.1 is used because it matches the real address best. We do not recommend using overlapping rules; they use more memory and can slow the performance of the security appliance.

## Mapped Address Guidelines

When you translate the real address to a mapped address, you can use the following mapped addresses:

- Addresses on the same network as the mapped interface.

If you use addresses on the same network as the mapped interface (through which traffic exits the security appliance), the security appliance uses proxy ARP to answer any requests for mapped addresses, and thus intercepts traffic destined for a real address. This solution simplifies routing, because the security appliance does not have to be the gateway for any additional networks. However, this approach does put a limit on the number of available addresses used for translations.

For PAT, you can even use the IP address of the mapped interface.

- Addresses on a unique network.

If you need more addresses than are available on the mapped interface network, you can identify addresses on a different subnet. The security appliance uses proxy ARP to answer any requests for mapped addresses, and thus intercepts traffic destined for a real address. If you use OSPF, and you advertise routes on the mapped interface, then the security appliance advertises the mapped addresses. If the mapped interface is passive (not advertising routes) or you are using static routing, then you need to add a static route on the upstream router that sends traffic destined for the mapped addresses to the security appliance.

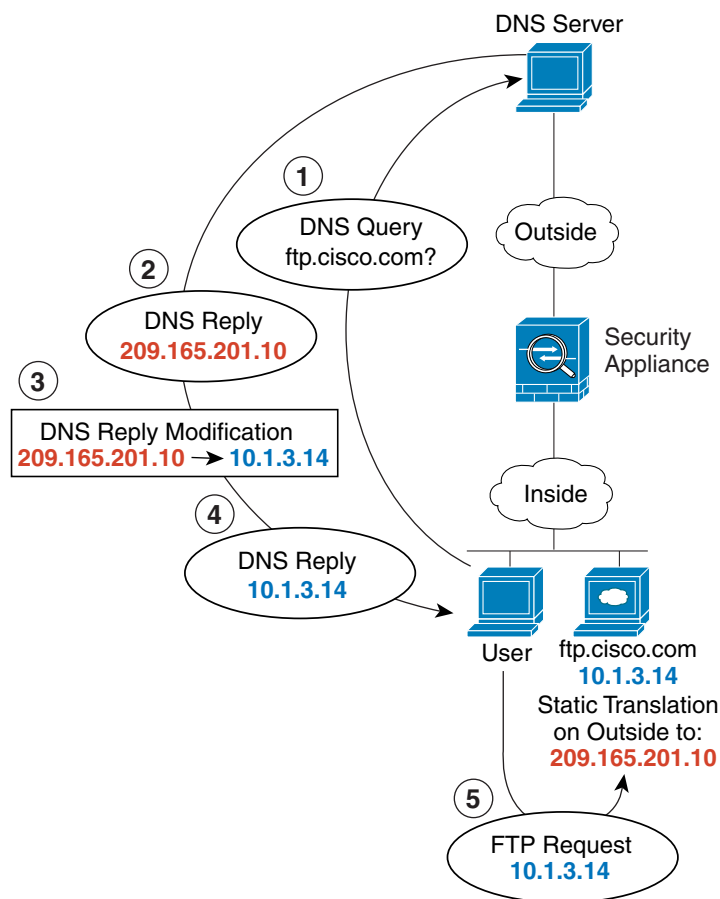
## DNS and NAT

You might need to configure the security appliance to modify DNS replies by replacing the address in the reply with an address that matches the NAT configuration. You can configure DNS modification when you configure each translation.

For example, a DNS server is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure the security appliance to statically translate the ftp.cisco.com real address (10.1.3.14) to a mapped address (209.165.201.10) that is visible on the outside network (see [Figure 21-12](#)). In this case, you want to enable DNS reply modification on this static statement so that inside users who have access to ftp.cisco.com using the real address receive the real address from the DNS server, and not the mapped address.

When an inside host sends a DNS request for the address of ftp.cisco.com, the DNS server replies with the mapped address (209.165.201.10). The security appliance refers to the static statement for the inside server and translates the address inside the DNS reply to 10.1.3.14. If you do not enable DNS reply modification, then the inside host attempts to send traffic to 209.165.201.10 instead of accessing ftp.cisco.com directly.

**Figure 21-12 DNS Reply Modification**



130021

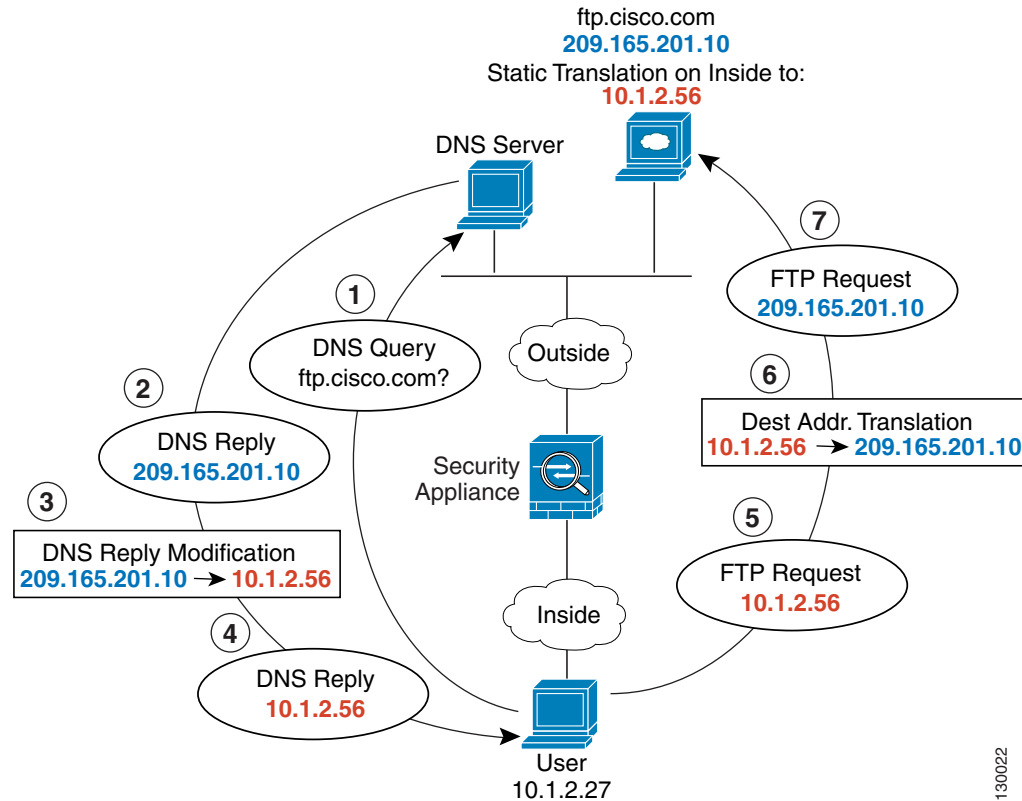


**Note**

If a user on a different network (for example, DMZ) also requests the IP address for ftp.cisco.com from the outside DNS server, then the IP address in the DNS reply is also modified for this user, even though the user is not on the Inside interface referenced by the static rule.

Figure 21-13 shows a web server and DNS server on the outside. The security appliance has a static translation for the outside server. In this case, when an inside user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.20.10. Because you want inside users to use the mapped address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.

**Figure 21-13** DNS Reply Modification Using Outside NAT



130022

## Configuring NAT Control

NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule. See the “NAT Control” section on page 21-4 for more information.

To enable NAT control, on the Configuration > Firewall > NAT Rules pane, check **Enable traffic through the firewall without address translation**.

# Using Dynamic NAT

This section describes how to configure dynamic NAT, including dynamic NAT and PAT, dynamic policy NAT and PAT, and identity NAT.

Policy NAT lets you identify real addresses for address translation by specifying the source and destination addresses. You can also optionally specify the source and destination ports. Regular NAT can only consider the source addresses, and not the destination. See the [“Policy NAT” section on page 21-10](#) for more information.

This section includes the following topics:

- [Dynamic NAT Implementation, page 21-16](#)
- [Managing Global Pools, page 21-21](#)
- [Configuring Dynamic NAT, PAT, or Identity NAT, page 21-22](#)
- [Configuring Dynamic Policy NAT or PAT, page 21-24](#)

## Dynamic NAT Implementation

This section describes how dynamic NAT is implemented, and includes the following topics:

- [Real Addresses and Global Pools Paired Using a Pool ID, page 21-17](#)
- [NAT Rules on Different Interfaces with the Same Global Pools, page 21-17](#)
- [Global Pools on Different Interfaces with the Same Pool ID, page 21-18](#)
- [Multiple NAT Rules with Different Global Pools on the Same Interface, page 21-18](#)
- [Multiple Addresses in the Same Global Pool, page 21-19](#)
- [Outside NAT, page 21-20](#)
- [Real Addresses in a NAT Rule Must be Translated on All Lower or Same Security Interfaces, page 21-21](#)



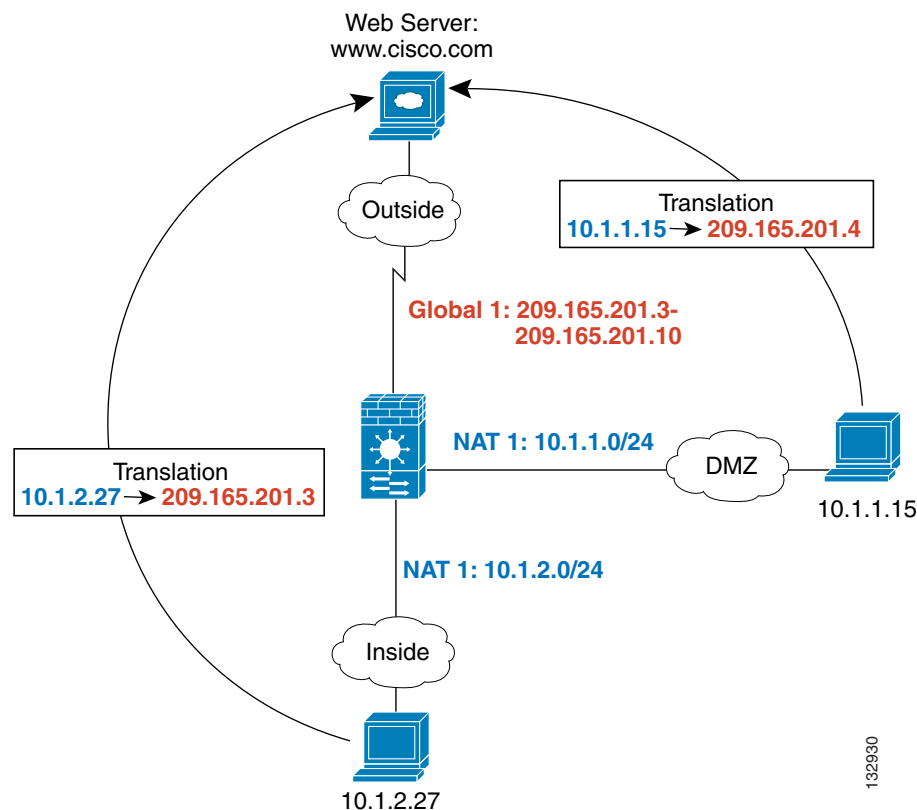
## Real Addresses and Global Pools Paired Using a Pool ID

In a dynamic NAT rule, you specify real addresses and then pair them with a global pool of addresses to which the real addresses are mapped when they exit another interface (in the case of PAT, this is one address, and in the case of identity NAT, this is the same as the real address). Each global pool is assigned a pool ID.

## NAT Rules on Different Interfaces with the Same Global Pools

You can create a NAT rule for each interface using the same global address pool. For example, you can configure NAT rules for Inside and DMZ interfaces, both using global pool 1 on the outside interface. Traffic from the Inside interface and the DMZ interface share a mapped pool or a PAT address when exiting the Outside interface (see Figure 21-14).

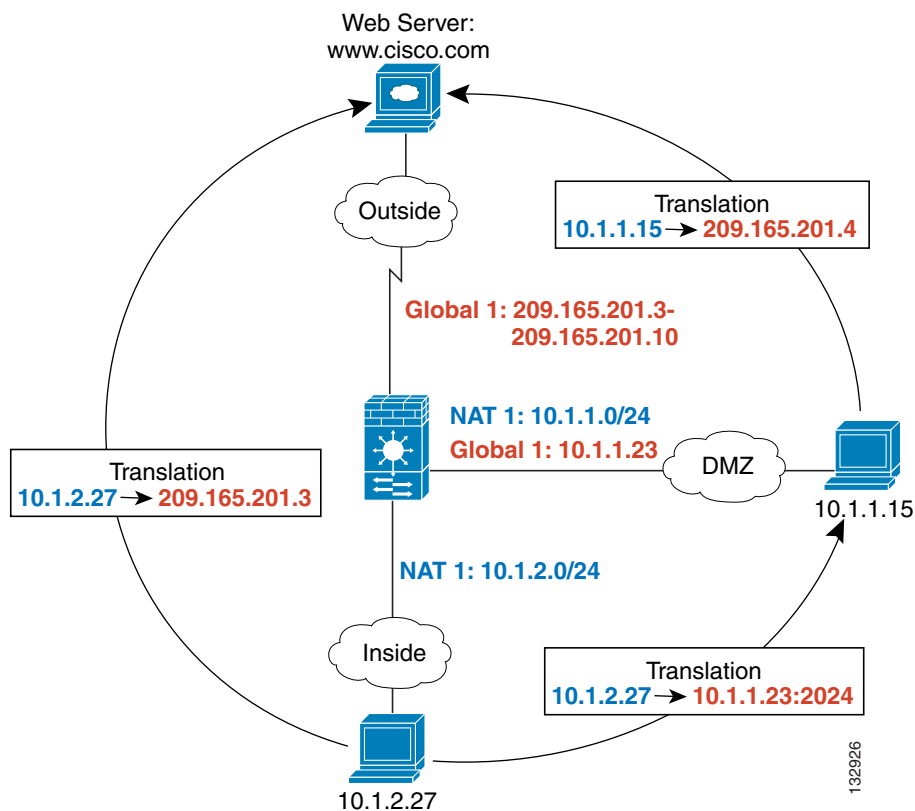
**Figure 21-14** NAT Rules on Multiple Interfaces Using the Same Global Pool



## Global Pools on Different Interfaces with the Same Pool ID

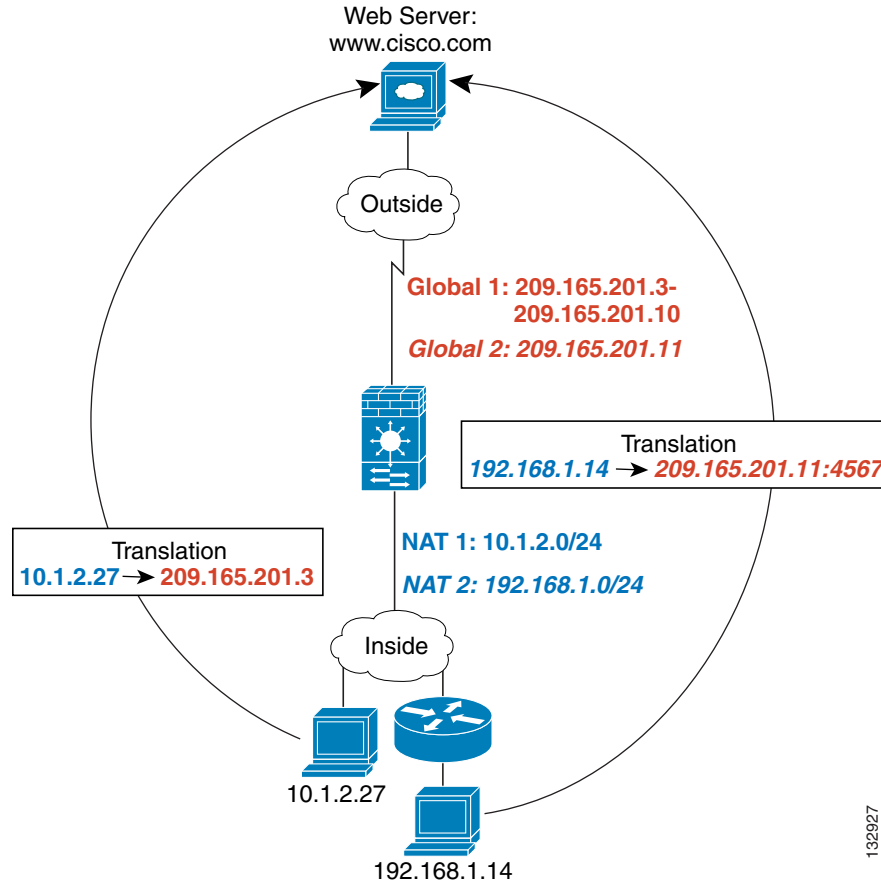
You can create a global pool for each interface using the same pool ID. If you create a global pool for the Outside and DMZ interfaces on ID 1, then a single NAT rule associated with ID 1 identifies traffic to be translated when going to both the Outside and the DMZ interfaces. Similarly, if you create a NAT rule for the DMZ interface on ID 1, then all global pools on ID 1 are also used for DMZ traffic. (See [Figure 21-15](#)).

**Figure 21-15** NAT Rules and Global Pools using the Same ID on Multiple Interfaces



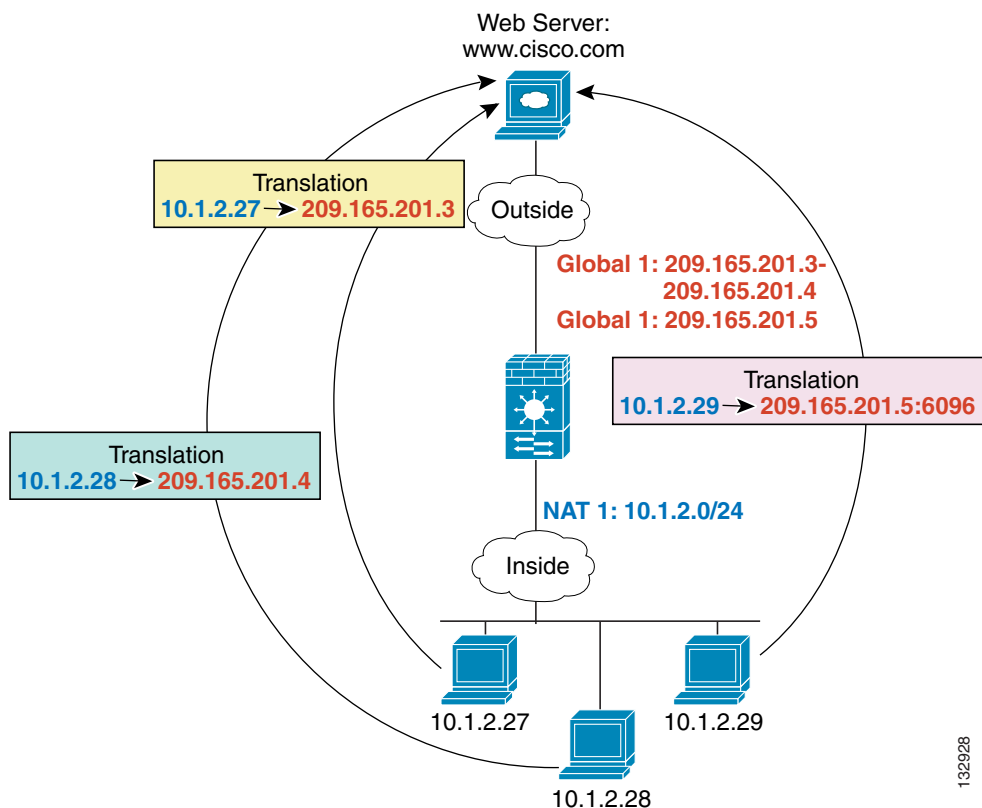
## Multiple NAT Rules with Different Global Pools on the Same Interface

You can identify different sets of real addresses to have different mapped addresses. For example, on the Inside interface, you can have two NAT rules on two different pool IDs. On the Outside interface, you configure two global pools for these two IDs. Then, when traffic from Inside network A exits the Outside interface, the IP addresses are translated to pool 1 addresses; while traffic from Inside network B are translated to pool 2 addresses (see [Figure 21-16](#)). If you use policy NAT, you can specify the same real addresses for multiple NAT rules, as long as the destination addresses and ports are unique in each access list.

**Figure 21-16** Different NAT IDs

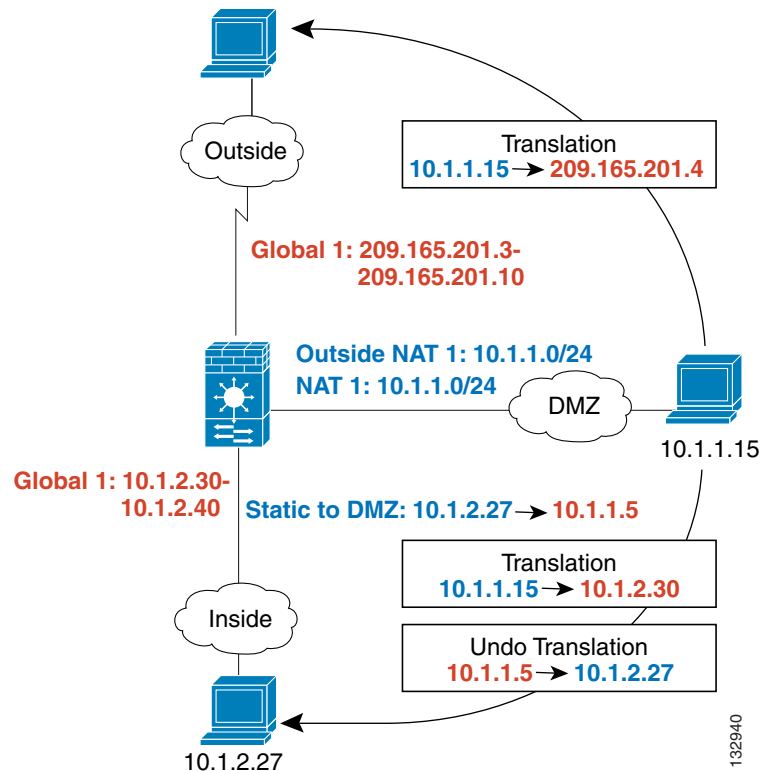
## Multiple Addresses in the Same Global Pool

You can have multiple addresses in the same global pool; the security appliance uses the dynamic NAT ranges of addresses first, in the order they are in the configuration, and then uses the PAT single addresses in order. You might want to add both a range of addresses and a PAT address if you need to use dynamic NAT for a particular application, but want to have a backup PAT rule in case all the dynamic NAT addresses are depleted. Similarly, you might want two PAT addresses in the pool if you need more than the approximately 64,000 PAT sessions that a single PAT mapped address supports (see [Figure 21-17](#)).

**Figure 21-17 NAT and PAT Together**

## Outside NAT

If a NAT rule translates addresses from an outside interface to an inside interface, then the rule is an outside NAT rule, and you need to specify that it translates inbound traffic. If you also want to translate the same traffic when it accesses a lower security interface (for example, traffic on a DMZ is translated when accessing the Inside and the Outside interfaces), then you can create a second NAT rule using the same NAT ID (see [Figure 21-18](#)), but specifying outbound. Note that for outside NAT (DMZ interface to Inside interface), the inside host uses a static rule to allow outside access, so both the source and destination addresses are translated.

**Figure 21-18** Outside NAT and Inside NAT Combined

## Real Addresses in a NAT Rule Must be Translated on All Lower or Same Security Interfaces

When you create a NAT rule for a group of IP addresses, then you must perform NAT on that group of addresses when they access any lower or same security level interface; you must create a global pool with the same pool ID on each interface, or use a static rule. NAT is not required for that group when it accesses a higher security interface. If you create an outside NAT rule, then the NAT requirements preceding come into effect for that group of addresses when they access all higher security interfaces. Traffic identified by a static rule is not affected.

## Managing Global Pools

Dynamic NAT uses global pools for translation. For information about how global pools work, see the [“Dynamic NAT Implementation”](#) section on page 21-16.

To manage a global pool, perform the following steps:

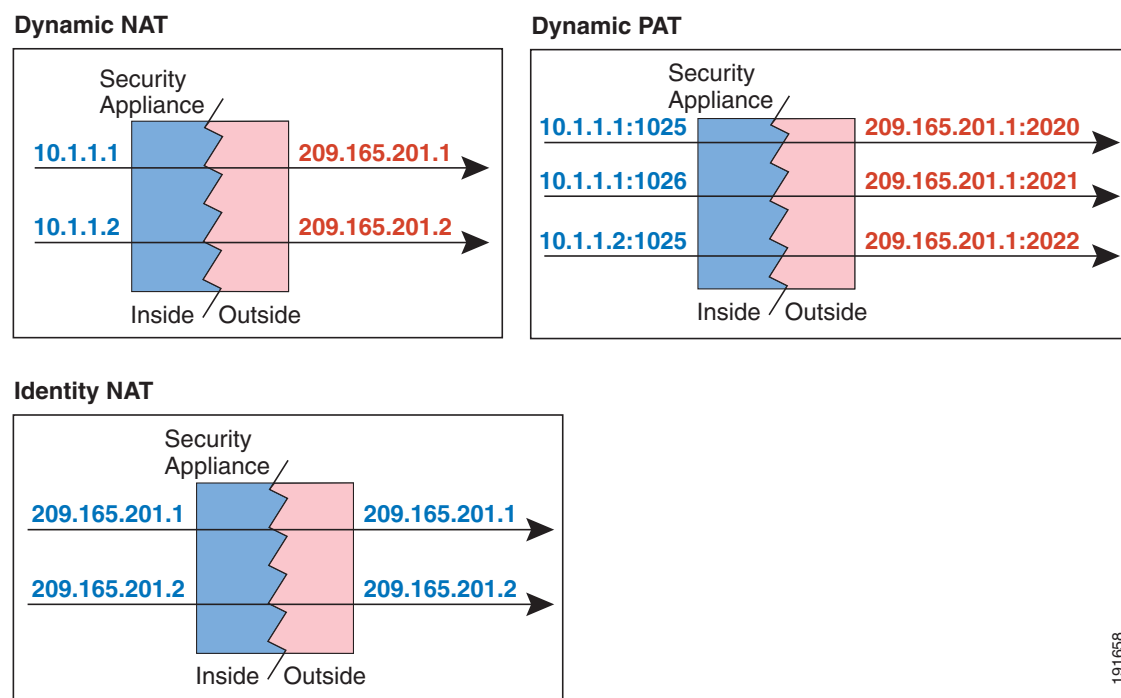
- Step 1** From the Configuration > Firewall > Objects > Global Pools pane, click **Add** to add a new pool, or choose a pool and click **Edit**.
- You can also manage global pools from the Add/Edit Dynamic NAT Rule dialog box by clicking the **Manage** button.
- The Add/Edit Global Address Pool dialog box appears.

- Step 2** For a new pool, from the Interface drop-down list, choose the interface where you want to use the mapped IP addresses.
- Step 3** For a new pool, in the Pool ID field, enter a number between 1 and 2147483647. Do not enter a pool ID that is already in use, or your configuration will be rejected.
- Step 4** In the IP Addresses to Add area, click **Range**, **Port Address Translation (PAT)**, or **PAT Address Translation (PAT) Using IP Address of the interface**.
- If you specify a range of addresses, the security appliance performs dynamic NAT. If you specify a subnet mask in the Netmask field, the value specifies the subnet mask assigned to the mapped address when it is assigned to a host. If you do not specify a mask, then the default mask for the address class is used.
- Step 5** Click **Add** to add the addresses to the Addresses Pool window.
- Step 6** (Optional) You can add multiple addresses to the global pool. If you want to add a PAT address after you configure a dynamic range, for example, then complete the value for PAT and click **Add** again. See the [“Multiple Addresses in the Same Global Pool”](#) section on page 21-19 for information about using multiple addresses on the same pool ID for an interface.
- Step 7** Click **OK**.

## Configuring Dynamic NAT, PAT, or Identity NAT

Figure 21-19 shows typical dynamic NAT, dynamic PAT, and identity NAT scenarios. Only real hosts can initiate connections.

**Figure 21-19** Dynamic NAT Scenarios



191658

To configure a dynamic NAT, PAT, or identity NAT rule, perform the following steps.

- 
- Step 1** From the Configuration > Firewall > NAT Rules pane, choose **Add > Add Dynamic NAT Rule**.  
The Add Dynamic NAT Rule dialog box appears.
- Step 2** In the Original area, from the Interface drop-down list, choose the interface that is connected to the hosts with real addresses that you want to translate.
- Step 3** Enter the real addresses in the Source field, or click the ... button to choose an IP address that you already defined in ASDM.  
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
- Step 4** To choose a global pool, use one of the following options:
- Choose an already-defined global pool.  
If the pool includes a range of addresses, then the security appliance performs dynamic NAT. If the pool includes a single address, then the security appliance performs dynamic PAT. If a pool includes both ranges and single addresses, then the ranges are used in order, and then the PAT addresses are used in order. See the [“Multiple Addresses in the Same Global Pool”](#) section on page 21-19 for more information.  
Pools are identified by a pool ID. If multiple global pools on different interfaces share the same pool ID, then they are grouped. If you choose a multi-interface pool ID, then traffic is translated as specified when it accesses any of the interfaces in the pool. For more information about pool IDs, see the [“Dynamic NAT Implementation”](#) section on page 21-16.
  - Create a new global pool or edit an existing pool by clicking **Manage**. See the [“Managing Global Pools”](#) section on page 21-21.
  - Choose identity NAT by choosing global pool 0.
- Step 5** (Optional) To enable translation of addresses inside DNS replies, click the **Connection Settings** area open, and check **Translate the DNS replies that match the translation rule**.  
If your NAT rule includes the real address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the mapped address and one needs the real address. This option rewrites the address in the DNS reply to the client. The mapped host needs to be on the same interface as either the client or the DNS server. Typically, hosts that need to allow access from other interfaces use a static translation, so this option is more likely to be used with a static rule. See the [“DNS and NAT”](#) section on page 21-13 for more information.
- Step 6** (Optional) To enable connection settings, click the **Connection Settings** area open, and set one or more of the following options:



**Note**

You can also set these values using a security policy rule (see the [“Configuring Connection Settings”](#) section on page 27-6). If you set them in both places, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

- Randomize sequence number**—With this check box checked (the default), the security appliance randomizes the sequence number of TCP packets. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

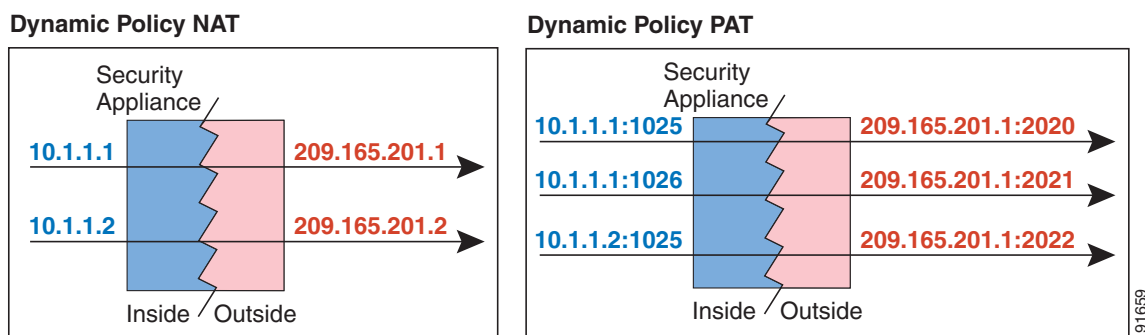
- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
  - If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
  - You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
- **Maximum TCP Connections**—Specifies the maximum number of TCP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum UDP Connections**—Specifies the maximum number of UDP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

**Step 7** Click OK.

## Configuring Dynamic Policy NAT or PAT

Figure 21-20 shows typical dynamic policy NAT and PAT scenarios. Only real hosts can initiate connections.

**Figure 21-20** Dynamic Policy NAT Scenarios





To configure dynamic policy NAT or PAT, perform the following steps:

- 
- Step 1** From the Configuration > Firewall > NAT Rules pane, choose **Add > Advanced > Add Dynamic Policy NAT Rule**.
- The Add Dynamic Policy NAT Rule dialog box appears.
- Step 2** In the Original area, from the Interface drop-down list, choose the interface that is connected to the hosts with real addresses that you want to translate.
- Step 3** Enter the real addresses in the Source field, or click the ... button to choose an IP address that you already defined in ASDM.
- Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
- Separate multiple real addresses by a comma.
- Step 4** Enter the destination addresses in the Destination field, or click the ... button to choose an IP address that you already defined in ASDM.
- Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
- Separate multiple destination addresses by a comma.
- By default, the field shows **any**, which allows any destination address.
- Step 5** To choose a global pool, use one of the following options:
- Choose an already-defined global pool.
- If the pool includes a range of addresses, then the security appliance performs dynamic NAT. If the pool includes a single address, then the security appliance performs dynamic PAT. If a pool includes both ranges and single addresses, then the ranges are used in order, and then the PAT addresses are used in order. See the [“Multiple Addresses in the Same Global Pool” section on page 21-19](#) for more information.
- Pools are identified by a pool ID. If multiple global pools on different interfaces share the same pool ID, then they are grouped. If you choose a multi-interface pool ID, then traffic is translated as specified when it accesses any of the interfaces in the pool. For more information about pool IDs, see the [“Dynamic NAT Implementation” section on page 21-16](#).
- Create a new global pool or edit an existing pool by clicking **Manage**. See the [“Managing Global Pools” section on page 21-21](#).
  - Choose identity NAT by choosing global pool 0.
- Step 6** (Optional) Enter a description in the Description field.
- Step 7** (Optional) To enable translation of addresses inside DNS replies, click the **Connection Settings** area open, and check **Translate the DNS replies that match the translation rule**.
- If your NAT rule includes the real address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the mapped address and one needs the real address. This option rewrites the address in the DNS reply to the client. The mapped host needs to be on the same interface as either the client or the DNS server. Typically, hosts that need to allow access from other interfaces use a static translation, so this option is more likely to be used with a static rule. See the [“DNS and NAT” section on page 21-13](#) for more information.
- Step 8** (Optional) To enable connection settings, click the **Connection Settings** area open, and set one or more of the following options:

**Note**

You can also set these values using a security policy rule (see the [“Configuring Connection Settings” section on page 27-6](#)). If you set them in both places, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

- **Randomize sequence number**—With this check box checked (the default), the security appliance randomizes the sequence number of TCP packets. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
  - If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
  - You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
- **Maximum TCP Connections**—Specifies the maximum number of TCP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum UDP Connections**—Specifies the maximum number of UDP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

**Step 9** Click **OK**.

## Using Static NAT

This section describes how to configure a static translation, using regular or policy static NAT, PAT, or identity NAT.

For more information about static NAT, see the [“Static NAT” section on page 21-8](#).

Policy NAT lets you identify real addresses for address translation by specifying the source and destination addresses. You can also optionally specify the source and destination ports. Regular NAT can only consider the source addresses, and not the destination. See the [“Policy NAT” section on page 21-10](#) for more information.

Static PAT lets you translate the real IP address to a mapped IP address, as well as the real port to a mapped port. You can choose to translate the real port to the same port, which lets you translate only specific types of traffic, or you can take it further by translating to a different port. For applications that require application inspection for secondary channels (for example, FTP and VoIP), the security appliance automatically translates the secondary ports. For more information about static PAT, see the [“Static PAT” section on page 21-9](#).

You cannot use the same real or mapped address in multiple static rules between the same two interfaces unless you use static PAT. Do not use a mapped address in the static rule that is also defined in a global pool for the same mapped interface.

Static identity NAT translates the real IP address to the same IP address.

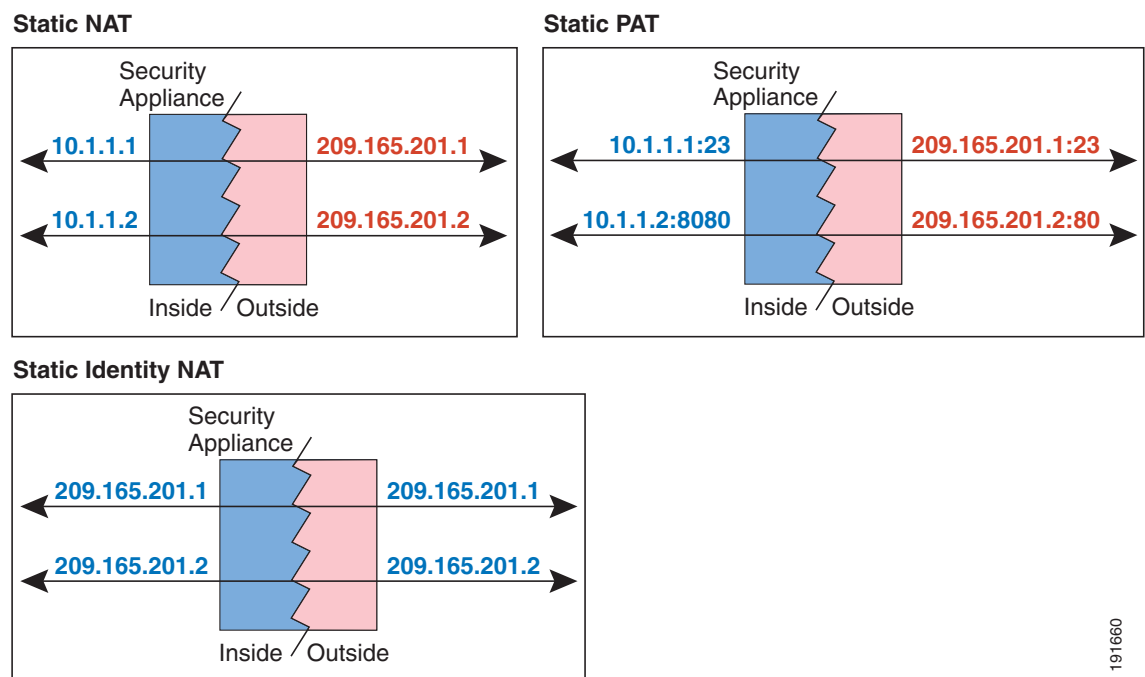
This section includes the following topics:

- [Configuring Static NAT, PAT, or Identity NAT, page 21-26](#)
- [Configuring Static Policy NAT, PAT, or Identity NAT, page 21-28](#)

## Configuring Static NAT, PAT, or Identity NAT

[Figure 21-21](#) shows typical static NAT, static PAT, and static identity NAT scenarios. The translation is always active so both translated and remote hosts can originate connections.

**Figure 21-21 Static NAT Scenarios**



To configure static NAT, PAT, or identity NAT, perform the following steps:

- Step 1** From the Configuration > Firewall > NAT Rules pane, choose **Add > Add Static NAT Rule**.  
The Add Static NAT Rule dialog box appears.
- Step 2** In the Original area, from the Interface drop-down list, choose the interface that is connected to the hosts with real addresses that you want to translate.
- Step 3** Enter the real addresses in the Source field, or click the ... button to choose an IP address that you already defined in ASDM.  
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
- Step 4** In the Translated area, from the Interface drop-down list, choose the interface where you want to use the mapped addresses.
- Step 5** Specify the mapped IP address by clicking one of the following:
- **Use IP Address**  
Enter the IP address or click the ... button to choose an IP address that you already defined in ASDM.  
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
  - **Use Interface IP Address**
- The real and mapped addresses must have the same subnet mask.



**Note** For identity NAT, enter the same IP address in the Original and Translated fields.

- Step 6** (Optional) To use static PAT, check **Enable Port Address Translation (PAT)**.
- a. For the Protocol, click **TCP** or **UDP**.
  - b. In the Original Port field, enter the real port number.
  - c. In the Translated Port field, enter the mapped port number.
- Step 7** (Optional) To enable translation of addresses inside DNS replies, click the **Connection Settings** area open, and check **Translate the DNS replies that match the translation rule**.  
If your NAT rule includes the real address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the mapped address and one needs the real address. This option rewrites the address in the DNS reply to the client. The mapped host needs to be on the same interface as either the client or the DNS server. See the [“DNS and NAT” section on page 21-13](#) for more information.
- Step 8** (Optional) To enable connection settings, click the **Connection Settings** area open, and set one or more of the following options:



**Note** You can also set these values using a security policy rule (see the [“Configuring Connection Settings” section on page 27-6](#)). If you set them in both places, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

- **Randomize sequence number**—With this check box checked (the default), the security appliance randomizes the sequence number of TCP packets. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
  - If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
  - You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
- **Maximum TCP Connections**—Specifies the maximum number of TCP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum UDP Connections**—Specifies the maximum number of UDP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
  - **Maximum Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

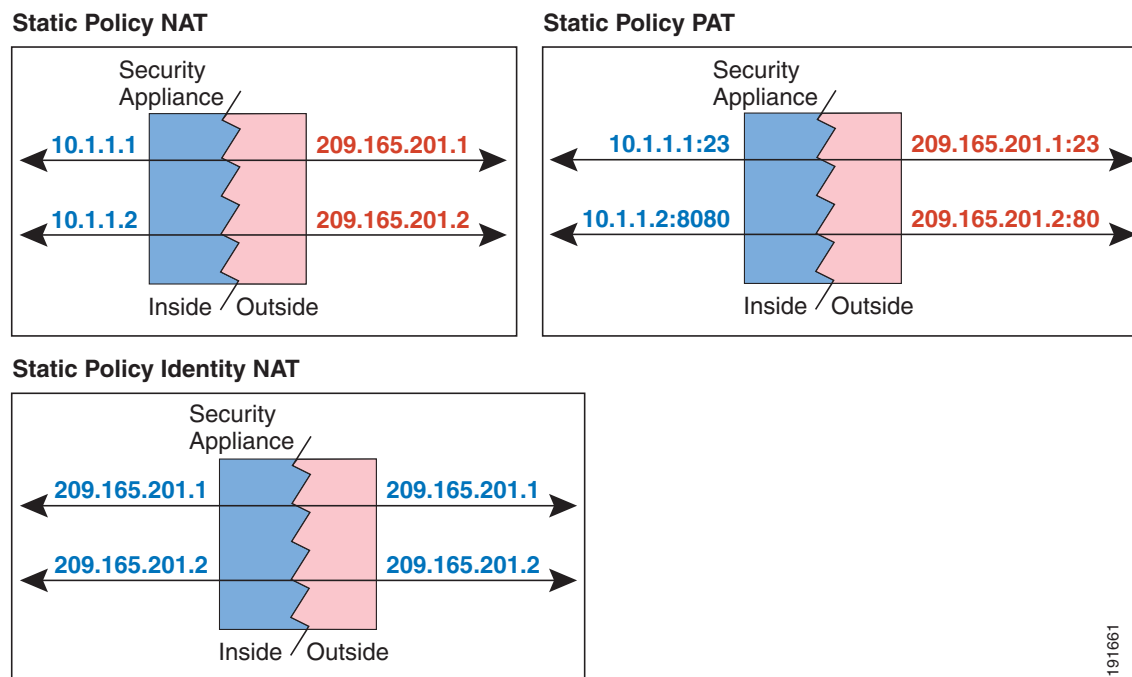
**Step 9** Click **OK**.

---

## Configuring Static Policy NAT, PAT, or Identity NAT

Figure 21-22 shows typical static policy NAT, static policy PAT, and static policy identity NAT scenarios. The translation is always active so both translated and remote hosts can originate connections.

**Figure 21-22** Static Policy NAT Scenarios



191661

To configure static policy NAT, PAT, or identity NAT, perform the following steps:

- Step 1** From the Configuration > Firewall > NAT Rules pane, choose **Add > Advanced > Add Static Policy NAT Rule**.  
The Add Static Policy NAT Rule dialog box appears.
- Step 2** In the Original area, from the Interface drop-down list, choose the interface that is connected to the hosts with real addresses that you want to translate.
- Step 3** Enter the real addresses in the Source field, or click the ... button to choose an IP address that you already defined in ASDM.  
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.
- Step 4** Enter the destination addresses in the Destination field, or click the ... button to choose an IP address that you already defined in ASDM.  
Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.  
Separate multiple destination addresses by a comma.  
By default, the field shows **any**, which allows any destination address.
- Step 5** In the Translated area, from the Interface drop-down list, choose the interface where you want to use the mapped addresses.

**Step 6** Specify the mapped IP address by clicking one of the following:

- **Use IP Address**

Enter the IP address or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

- **Use Interface IP Address**

The real and mapped addresses must have the same subnet mask.

**Step 7** (Optional) To use static PAT, check **Enable Port Address Translation (PAT)**.

- For the Protocol, click **TCP** or **UDP**.
- In the Original Port field, enter the real port number.
- In the Translated Port field, enter the mapped port number.

**Step 8** (Optional) Enter a description in the Description field.

**Step 9** (Optional) To enable translation of addresses inside DNS replies, click the **Connection Settings** area open, and check **Translate the DNS replies that match the translation rule**.

If your NAT rule includes the real address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the mapped address and one needs the real address. This option rewrites the address in the DNS reply to the client. The mapped host needs to be on the same interface as either the client or the DNS server. See the [“DNS and NAT” section on page 21-13](#) for more information.

**Step 10** (Optional) To enable connection settings, click the **Connection Settings** area open, and set one or more of the following options:



**Note**

You can also set these values using a security policy rule (see the [“Configuring Connection Settings” section on page 27-6](#)). If you set them in both places, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

- **Randomize sequence number**—With this check box checked (the default), the security appliance randomizes the sequence number of TCP packets. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predefining the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.

- **Maximum TCP Connections**—Specifies the maximum number of TCP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.
- **Maximum UDP Connections**—Specifies the maximum number of UDP connections, between 0 and 65,535. If this value is set to 0, the number of connections is unlimited.

- **Maximum Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

**Step 11** Click **OK**.

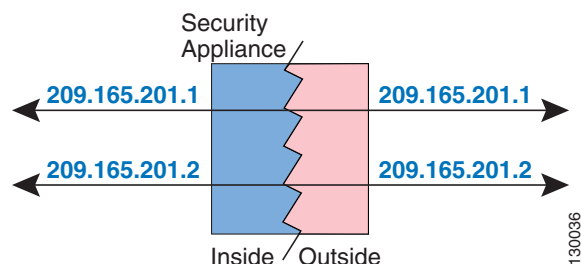
## Using NAT Exemption

NAT exemption exempts addresses from translation and allows both real and remote hosts to originate connections. NAT exemption lets you specify the real and destination addresses when determining the real traffic to exempt (similar to policy NAT), so you have greater control using NAT exemption than dynamic identity NAT. However unlike policy NAT, NAT exemption does not consider the ports. Use static policy identity NAT to consider ports.

For more information about NAT exemption, see the [“Bypassing NAT When NAT Control is Enabled” section on page 21-10](#).

Figure 21-23 shows a typical NAT exemption scenario.

**Figure 21-23 NAT Exemption**



To configure NAT exemption, perform the following steps:

- Step 1** From the Configuration > Firewall > NAT Rules pane, choose **Add > Add NAT Exempt Rule**. The Add NAT Exempt Rule dialog box appears.
- Step 2** Click **Action: Exempt**.
- Step 3** In the Original area, from the Interface drop-down list, choose the interface that is connected to the hosts with real addresses that you want to exempt.
- Step 4** Enter the real addresses in the Source field, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.



**Note**

You can later specify addresses that you do not want to exempt. For example, you can specify a subnet to exempt such as 10.1.1.0/24, but if you want to translate 10.1.1.50, then you can create a separate rule for that address that removes the exemption.

Separate multiple real addresses by a comma.

- Step 5** Enter the destination addresses in the Destination field, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Separate multiple destination addresses by a comma.

By default, the field shows **any**, which allows any destination address.

- Step 6** In the NAT Exempt Direction area, choose whether you want to exempt traffic going to lower security interfaces (the default) or to higher security interfaces by clicking the appropriate radio button.

- Step 7** (Optional) Enter a description in the Description field.

- Step 8** Click **OK**.

- Step 9** (Optional) If you do not want to exempt some addresses that were included in your NAT exempt rule, then create another rule to remove the exemption. Right-click the existing NAT Exempt rule, and choose **Insert**.

The Add NAT Exempt Rule dialog box appears.

- a. Click **Action: Do not exempt**.
- b. Complete steps 3 through 8 to complete the rule.

The No Exempt rule is added before the Exempt rule. The order of Exempt and No Exempt rules is important. When the security appliance decides whether to exempt a packet, the security appliance tests the packet against each NAT exempt and No Exempt rule in the order in which the rules are listed. After a match is found, no more rules are checked.





## CHAPTER 22

# Configuring Service Policy Rules

---

This chapter describes how to enable service policy rules. Service policies provide a consistent and flexible way to configure security appliance features. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications.

This chapter includes the following sections:

- [Service Policy Overview, page 22-1](#)
- [Adding a Service Policy Rule for Through Traffic, page 22-6](#)
- [Adding a Service Policy Rule for Management Traffic, page 22-10](#)
- [Managing the Order of Service Policy Rules, page 22-13](#)
- [RADIUS Accounting Field Descriptions, page 22-14](#)

## Service Policy Overview

This section describes how security policies work, and includes the following topics:

- [Supported Features, page 22-1](#)
- [Service Policy Elements, page 22-2](#)
- [Default Global Policy, page 22-2](#)
- [Feature Directionality, page 22-3](#)
- [Order in Which Multiple Feature Actions within a Rule are Applied, page 22-4](#)
- [Order in Which Multiple Feature Actions within a Rule are Applied, page 22-4](#)

## Supported Features

Security policies support the following features:

- QoS input policing
- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization
- CSC
- Application inspection

- IPS
- QoS output policing
- QoS priority queue
- QoS traffic shaping, hierarchical priority queue
- NetFlow

## Service Policy Elements

Configuring a service policy consists of adding one or more service policy rules per interface or for the global policy. For each rule, you identify the following elements:

1. Identify the interface to which you want to apply the rule, or identify the global policy.
2. Identify the traffic to which you want to apply actions. You can identify Layer 3 and 4 through traffic.
3. Apply actions to the traffic class. You can apply multiple actions for each traffic class.

## Default Global Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy.)

The default policy includes the following application inspections:

- DNS inspection for the maximum message length of 512 bytes
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

## Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions.



### Note

When you use a global policy, all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally. Because the policy is applied to all interfaces, the policy will be applied in both directions so bidirectionality in this case is redundant.

For features that are applied unidirectionally, for example QoS priority queue, only traffic that exits the interface to which you apply the policy map is affected. See [Table 22-1](#) for the directionality of each feature.

**Table 22-1 Feature Directionality**

| Feature                                                                                              | Single Interface Direction | Global Direction |
|------------------------------------------------------------------------------------------------------|----------------------------|------------------|
| QoS input policing                                                                                   | Ingress                    | Ingress          |
| TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization | Bidirectional              | Ingress          |
| CSC                                                                                                  | Bidirectional              | Ingress          |
| Application inspection                                                                               | Bidirectional              | Ingress          |
| IPS                                                                                                  | Bidirectional              | Ingress          |
| QoS output policing                                                                                  | Egress                     | Egress           |
| QoS priority queue                                                                                   | Egress                     | Egress           |
| QoS traffic shaping, hierarchical priority queue                                                     | Egress                     | Egress           |
| NetFlow                                                                                              | Bidirectional              | Ingress          |

## Feature Matching Guidelines

See the following guidelines for how a packet matches rules for a given interface or for the global policy:

1. A packet can match only one rule for each feature type.
2. When the packet matches a rule for a feature type, the security appliance does not attempt to match it to any subsequent rules for that feature type.
3. If the packet matches a subsequent rule for a different feature type, however, then the security appliance also applies the actions for the subsequent rule, if supported. See the [“Incompatibility of Certain Feature Actions” section on page 22-5](#) for more information about unsupported combinations.

For example, if a packet matches a rule for connection limits, and also matches a rule for application inspection, then both rule actions are applied.

If a packet matches a rule for HTTP inspection, but also matches another rule that includes HTTP inspection, then the second rule actions are not applied.

**Note**

Application inspection includes multiple inspection types, and each inspection type is a separate feature when you consider the matching guidelines above.

## Order in Which Multiple Feature Actions within a Rule are Applied

The order in which different types of actions in a service policy are performed is independent of the order in which the actions appear in ASDM. Actions are performed in the following order:

1. QoS input policing
2. TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization

**Note**

When a the security appliance performs a proxy service (such as AAA or CSC) or it modifies the TCP payload (such as FTP inspection), the TCP normalizer acts in dual mode, where it is applied before and after the proxy or payload modifying service.

3. CSC
4. Application inspection (multiple types)

The order of application inspections applied when a class of traffic is classified for multiple inspections is as follows. Only one inspection type can be applied to the same traffic. WAAS inspection is an exception, because it can be applied along with other inspections for the same traffic. See the [“Incompatibility of Certain Feature Actions” section on page 22-5](#) for more information.

- a. CTIQBE
- b. DNS
- c. FTP
- d. GTP
- e. H323
- f. HTTP
- g. ICMP
- h. ICMP error
- i. ILS
- j. MGCP
- k. NetBIOS
- l. PPTP
- m. Sun RPC
- n. RSH
- o. RTSP
- p. SIP
- q. Skinny
- r. SMTP

- s. SNMP
- t. SQL\*Net
- u. TFTP
- v. XDMCP
- w. DCERPC
- x. Instant Messaging



**Note** RADIUS accounting is not listed because it is the only inspection allowed on management traffic. WAAS is not listed because it can be configured along with other inspections for the same traffic.

- 5. IPS
- 6. QoS output policing
- 7. QoS standard priority queue
- 8. QoS traffic shaping, hierarchical priority queue
- 9. NetFlow

## Incompatibility of Certain Feature Actions

Some features are not compatible with each other for the same traffic. For example, most inspections should not be combined with another inspection, so the security appliance only applies one inspection if you configure multiple inspections for the same traffic. In this case, the feature that is applied is the higher priority feature in the list in the [“Order in Which Multiple Feature Actions are Applied”](#) section on page 15-18.

For information about compatibility of each feature, see the chapter or section for your feature.



**Note**

The Default Inspection Traffic traffic classification, which is used in the default global policy, is a special shortcut to match the default ports for all inspections. When used in a rule, this traffic classification ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69 reaches the security appliance, then the security appliance applies the TFTP inspection; when TCP traffic for port 21 arrives, then the security appliance applies the FTP inspection. So in this case only, you can configure multiple inspections for the same rule. Normally, the security appliance does not use the port number to determine the inspection applied, thus giving you the flexibility to apply inspections to non-standard ports, for example.

## Feature Matching Guidelines for Multiple Service Policies

For TCP and UDP traffic (and ICMP when you enable stateful ICMP inspection), service policies operate on traffic flows, and not just individual packets. If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.

For example, if HTTP traffic matches a policy on the inside interface to inspect HTTP traffic, and you have a separate policy on the outside interface for HTTP inspection, then that traffic is not also inspected on the egress of the outside interface. Similarly, the return traffic for that connection will not be inspected by the ingress policy of the outside interface, nor by the egress policy of the inside interface.

For traffic that is not treated as a flow, for example ICMP when you do not enable stateful ICMP inspection, returning traffic can match a different policy map on the returning interface. For example, if you configure IPS inspection on the inside and outside interfaces, but the inside policy uses virtual sensor 1 while the outside policy uses virtual sensor 2, then a non-stateful Ping will match virtual sensor 1 outbound, but will match virtual sensor 2 inbound.

## Adding a Service Policy Rule for Through Traffic

To add a service policy rule for through traffic, perform the following steps:

**Step 1** From the Configuration > Firewall > Service Policy Rules pane, click **Add**.

The Add Service Policy Rule Wizard - Service Policy dialog box appears.



**Note** When you click the Add button, and not the small arrow on the right of the Add button, you add a through traffic rule by default. If you click the arrow on the Add button, you can choose between a through traffic rule and a management traffic rule.

**Step 2** In the Create a Service Policy and Apply To area, click one of the following options:

- **Interface.** This option applies the service policy to a single interface. Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with FTP inspection, and an interface policy with TCP connection limits, then both FTP inspection and TCP connection limits are applied to the interface. However, if you have a global policy with FTP inspection, and an interface policy with FTP inspection, then only the interface policy FTP inspection is applied to that interface.
  - a. Choose an interface from the drop-down list.
 

If you choose an interface that already has a policy, then the wizard lets you add a new service policy rule to the interface.
  - b. If it is a new service policy, enter a name in the Policy Name field.
  - c. (Optional) Enter a description in the Description field.
- **Global - applies to all interfaces.** This option applies the service policy globally to all interfaces. By default, a global policy exists that includes a service policy rule for default application inspection. See the [“Default Global Policy”](#) section on page 22-2 for more information. You can add a rule to the global policy using the wizard.

**Step 3** Click **Next**.

The Add Service Policy Rule Wizard - Traffic Classification Criteria dialog box appears.

**Step 4** Click one of the following options to specify the traffic to which to apply the policy actions:

- **Create a new traffic class.** Enter a traffic class name in the Create a new traffic class field, and enter an optional description.

Identify the traffic using one of several criteria:



- **Default Inspection Traffic**—The class matches the default TCP and UDP ports used by all applications that the security appliance can inspect.

This option, which is used in the default global policy, is a special shortcut that when used in a rule, ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69 reaches the security appliance, then the security appliance applies the TFTP inspection; when TCP traffic for port 21 arrives, then the security appliance applies the FTP inspection. So in this case only, you can configure multiple inspections for the same rule (See the [“Incompatibility of Certain Feature Actions” section on page 22-5](#) for more information about combining actions). Normally, the security appliance does not use the port number to determine the inspection applied, thus giving you the flexibility to apply inspections to non-standard ports, for example.

See the [“Default Inspection Policy” section on page 24-3](#) for a list of default ports. The security appliance includes a default global policy that matches the default inspection traffic, and applies common inspections to the traffic on all interfaces. Not all applications whose ports are included in the Default Inspection Traffic class are enabled by default in the policy map.

You can specify a Source and Destination IP Address (uses ACL) class along with the Default Inspection Traffic class to narrow the matched traffic. Because the Default Inspection Traffic class specifies the ports to match, any ports in the access list are ignored.

- **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended access list. If the security appliance is operating in transparent firewall mode, you can use an EtherType access list.



**Note** When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** on the Traffic Classification dialog box (see below).

- **Tunnel Group**—The class matches traffic for a tunnel group to which you want to apply QoS. You can also specify one other traffic match option to refine the traffic match, excluding Any Traffic, Source and Destination IP Address (uses ACL), or Default Inspection Traffic.
- **TCP or UDP Destination Port**—The class matches a single port or a contiguous range of ports.



**Tip**

For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- **RTP Range**—The class map matches RTP traffic.
- **IP DiffServ CodePoints (DSCP)**—The class matches up to eight DSCP values in the IP header.
- **IP Precedence**—The class map matches up to four precedence values, represented by the TOS byte in the IP header.
- **Any Traffic**—Matches all traffic.
- **Add rule to existing traffic class.** If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing access list. You can add an ACE to any access list that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add

multiple ACEs to the same traffic class by repeating this entire procedure. See the [“Managing the Order of Service Policy Rules” section on page 22-13](#) for information about changing the order of ACEs.

- **Use an existing traffic class.** If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any **class-map** commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).
- **Use class default as the traffic class.** This option uses the class-default class, which matches all traffic. The class-default class is created automatically by the security appliance and placed at the end of the policy. If you do not apply any actions to it, it is still created by the security appliance, but for internal purposes only. You can apply actions to this class, if desired, which might be more convenient than creating a new traffic class that matches all traffic. You can only create one rule for this service policy using the class-default class, because each traffic class can only be associated with a single rule per service policy.

**Step 5** Click **Next**.

**Step 6** The next dialog box depends on the traffic match criteria you chose.



**Note** The Any Traffic option does not have a special dialog box for additional configuration.

- **Default Inspections**—This dialog box is informational only, and shows the applications and the ports that are included in the traffic class.
- **Source and Destination Address**—This dialog box lets you set the source and destination addresses:

**a. Click **Match** or **Do Not Match**.**

The Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.

**b. In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.**

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any source address.

Separate multiple addresses by a comma.

**c. In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.**

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any destination address.

Separate multiple addresses by a comma.

**d. In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.**

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.

By default, the service is IP.

Separate multiple services by a comma.

- e. (Optional) Enter a description in the Description field.
- f. (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.

- g. (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.

- h. (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the [“Configuring Time Ranges” section on page 19-15](#) for more information.

This setting might be useful if you only want the rule to be active at predefined times.

- Tunnel Group—Choose a tunnel group from the Tunnel Group drop-down list, or click **New** to add a new tunnel group. See the [“IPSec Remote Access Connection Profiles” section on page 35-49](#) for more information.

To police each flow, check **Match flow destination IP address**. All traffic going to a unique IP destination address is considered a flow.

- Destination Port—Click **TCP** or **UDP**.

In the Service field, enter a port number or name, or click ... to choose one already defined in ASDM.

- RTP Range—Enter an RTP port range, between 2000 and 65534. The maximum number of port sin the range is 16383.
- IP DiffServ CodePoints (DSCP)—In the DSCP Value to Add area, choose a value from the **Select Named DSCP Values** or enter a value in the **Enter DSCP Value (0-63)** field, and click **Add**.

Add additional values as desired, or remove them using the **Remove** button.

- IP Precedence—From the Available IP Precedence area, choose a value and click **Add**.

Add additional values as desired, or remove them using the **Remove** button.

**Step 7** Click **Next**.

The Add Service Policy Rule - Rule Actions dialog box appears.

**Step 8** Configure one or more rule actions according to the following sections:

- [Chapter 24, “Configuring Application Layer Protocol Inspection.”](#)
- [“Configuring Connection Settings” section on page 27-6](#)
- [Chapter 25, “Configuring QoS.”](#)
- [Chapter 28, “Configuring IPS.”](#)
- [Chapter 29, “Configuring Trend Micro Content Security.”](#)
- [Chapter 24, “Configuring MMP Inspection for a TLS Proxy”](#)
- [“Matching NetFlow Events to Configured Collectors” section on page 17-19](#)

**Step 9** Click **Finish**.

---

## Adding a Service Policy Rule for Management Traffic

You can create a service policy for traffic directed to the security appliance for management purposes. This type of security policy can perform RADIUS accounting inspection and connection limits. This section includes the following topics:

- [RADIUS Accounting Inspection Overview, page 22-10](#)
- [Configuring a Service Policy Rule for Management Traffic, page 22-10](#)

## RADIUS Accounting Inspection Overview

One of the well known problems is the over-billing attack in GPRS networks. The over-billing attack can cause consumers anger and frustration by being billed for services that they have not used. In this case, a malicious attacker sets up a connection to a server and obtains an IP address from the SGSN. When the attacker ends the call, the malicious server will still send packets to it, which gets dropped by the GGSN, but the connection from the server remains active. The IP address assigned to the malicious attacker gets released and reassigned to a legitimate user who will then get billed for services that the attacker will use.

RADIUS accounting inspection prevents this type of attack using by ensuring the traffic seen by the GGSN is legitimate. With the RADIUS accounting feature properly configured, the security appliance tears down a connection based on matching the Framed IP attribute in the Radius Accounting Request Start message with the Radius Accounting Request Stop message. When the Stop message is seen with the matching IP address in the Framed IP attribute, the security appliance looks for all connections with the source matching the IP address.

You have the option to configure a secret pre-shared key with the RADIUS server so the security appliance can validate the message. If the shared secret is not configured, the security appliance does not need to validate the source of the message and will only check that the source IP address is one of the configured addresses allowed to send the RADIUS messages.

## Configuring a Service Policy Rule for Management Traffic

To add a service policy rule for management traffic, perform the following steps:

- 
- Step 1** From the Configuration > Firewall > Service Policy Rules pane, click the down arrow next to Add.
- Step 2** Choose **Add Management Service Policy Rule**.  
The Add Management Service Policy Rule Wizard - Service Policy dialog box appears.
- Step 3** In the Create a Service Policy and Apply To area, click one of the following options:
- **Interface.** This option applies the service policy to a single interface. Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with RADIUS accounting inspection, and an interface policy with connection limits, then

both RADIUS accounting and connection limits are applied to the interface. However, if you have a global policy with RADIUS accounting, and an interface policy with RADIUS accounting, then only the interface policy RADIUS accounting is applied to that interface.

- a. Choose an interface from the drop-down list.

If you choose an interface that already has a policy, then the wizard lets you add a new service policy rule to the interface.

- b. If it is a new service policy, enter a name in the Policy Name field.

- c. (Optional) Enter a description in the Description field.

- **Global - applies to all interfaces.** This option applies the service policy globally to all interfaces. By default, a global policy exists that includes a service policy rule for default application inspection. See the [“Default Global Policy” section on page 22-2](#) for more information. You can add a rule to the global policy using the wizard.

**Step 4** Click **Next**.

The Add Management Service Policy Rule Wizard - Traffic Classification Criteria dialog box appears.

**Step 5** Click one of the following options to specify the traffic to which to apply the policy actions:

- **Create a new traffic class.** Enter a traffic class name in the Create a new traffic class field, and enter an optional description.

Identify the traffic using one of several criteria:

- **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended access list. If the security appliance is operating in transparent firewall mode, you can use an EtherType access list.



**Note**

When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** on the Traffic Classification dialog box (see below).

- **TCP or UDP Destination Port**—The class matches a single port or a contiguous range of ports.



**Tip**

For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- **Add rule to existing traffic class.** If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing access list. You can add an ACE to any access list that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add multiple ACEs to the same traffic class by repeating this entire procedure. See the [“Managing the Order of Service Policy Rules” section on page 22-13](#) for information about changing the order of ACEs.
- **Use an existing traffic class.** If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any **class-map** commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).

**Step 6** Click **Next**.

**Step 7** The next dialog box depends on the traffic match criteria you chose.

- Source and Destination Address—This dialog box lets you set the source and destination addresses:

- a. Click **Match** or **Do Not Match**.

The Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.

- b. In the Source field, enter the source IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any source address.

Separate multiple addresses by a comma.

- c. In the Destination field, enter the destination IP address, or click the ... button to choose an IP address that you already defined in ASDM.

Specify the address and subnet mask using prefix/length notation, such as 10.1.1.0/24. If you enter an IP address without a mask, it is considered to be a host address, even if it ends with a 0.

Enter **any** to specify any destination address.

Separate multiple addresses by a comma.

- d. In the Service field, enter an IP service name or number for the destination service, or click the ... button to choose a service.

If you want to specify a TCP or UDP port number, or an ICMP service number, enter *protocol/port*. For example, enter TCP/8080.

By default, the service is IP.

Separate multiple services by a comma.

- e. (Optional) Enter a description in the Description field.
- f. (Optional) To specify a source service for TCP or UDP, click the **More Options** area open, and enter a TCP or UDP service in the Source Service field.

The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.

- g. (Optional) To make the rule inactive, click the **More Options** area open, and uncheck **Enable Rule**.

This setting might be useful if you do not want to remove the rule, but want to turn it off.

- h. (Optional) To set a time range for the rule, click the **More Options** area open, and from the Time Range drop-down list, choose a time range.

To add a new time range, click the ... button. See the [“Configuring Time Ranges” section on page 19-15](#) for more information.

This setting might be useful if you only want the rule to be active at predefined times.

- Destination Port—Click **TCP** or **UDP**.

In the Service field, enter a port number or name, or click ... to choose one already defined in ASDM.

**Step 8** Click **Next**.

The Add Management Service Policy Rule - Rule Actions dialog box appears.

**Step 9** To configure RADIUS accounting inspection, choose an inspect map from the RADIUS Accounting Map drop-down list, or click **Configure** to add a map.

See the [“RADIUS Accounting Field Descriptions” section on page 22-14](#) for more information.

**Step 10** To configure maximum connections, enter one or more of the following values in the Maximum Connections area:

- **TCP & UDP Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for all clients in the traffic class, up to 65,536. The default is 0 for both protocols, which means the maximum possible connections are allowed.
- **Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.

**Step 11** Click **Finish**.

---

## Managing the Order of Service Policy Rules

The order of service policy rules on an interface or in the global policy affects how actions are applied to traffic. See the following guidelines for how a packet matches rules in a service policy:

- A packet can match only one rule in a service policy for each feature type.
- When the packet matches a rule that includes actions for a feature type, the security appliance does not attempt to match it to any subsequent rules including that feature type.
- If the packet matches a subsequent rule for a different feature type, however, then the security appliance also applies the actions for the subsequent rule.

For example, if a packet matches a rule for connection limits, and also matches a rule for application inspection, then both rule actions are applied.

If a packet matches a rule for application inspection, but also matches another rule that includes application inspection, then the second rule actions are not applied.

If your rule includes an access list with multiple ACEs, then the order of ACEs also affects the packet flow. The FWSM tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are ever checked.

To change the order of rules or ACEs within a rule, perform the following steps:

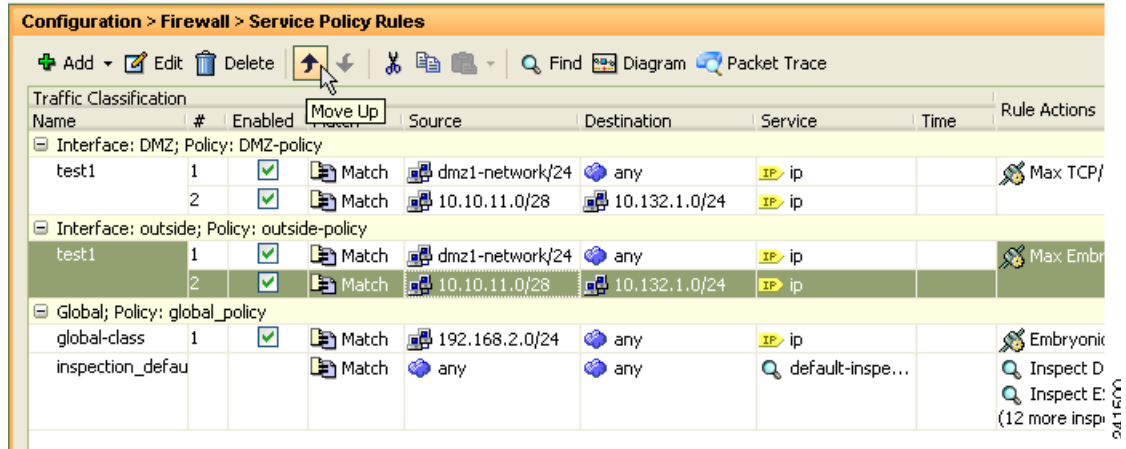
---

**Step 1** From the Configuration > Firewall > Service Policy Rules pane, choose the rule or ACE that you want to move up or down.



**Step 2** Click the Move Up or Move Down cursor (see [Figure 22-1](#)).

**Figure 22-1** Moving an ACE



**Note** If you rearrange ACEs in an access list that is used in multiple service policies, then the change is inherited in all service policies.

**Step 3** When you are done rearranging your rules or ACEs, click **Apply**.

## RADIUS Accounting Field Descriptions

This section lists RADIUS accounting field descriptions, and includes the following topics:

- [Select RADIUS Accounting Map, page 22-14](#)
- [Add RADIUS Accounting Policy Map, page 22-15](#)
- [RADIUS Inspect Map, page 22-16](#)
- [RADIUS Inspect Map Host, page 22-16](#)
- [RADIUS Inspect Map Other, page 22-17](#)

### Select RADIUS Accounting Map

The Select RADIUS Accounting Map dialog box lets you select a defined RADIUS accounting map or define a new one.

#### Fields

- **Add**—Lets you add a new RADIUS accounting map.

#### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add RADIUS Accounting Policy Map

The Add RADIUS Accounting Policy Map dialog box lets you add the basic settings for the RADIUS accounting map.

### Fields

- Name—Enter the name of the previously configured RADIUS accounting map.
- Description—Enter the description of the RADIUS accounting map, up to 100 characters in length.
- Host Parameters tab:
  - Host IP Address—Specify the IP address of the host that is sending the RADIUS messages.
  - Key: (optional)—Specify the key.
  - Add—Adds the host entry to the Host table.
  - Delete—Deletes the host entry from the Host table.
- Other Parameters tab:
  - Attribute Number—Specify the attribute number to validate when an Accounting Start is received.
  - Add—Adds the entry to the Attribute table.
  - Delete—Deletes the entry from the Attribute table.
  - Send response to the originator of the RADIUS message—Sends a message back to the host from which the RADIUS message was sent.
  - Enforce timeout—Enables the timeout for users.
- Users Timeout—Timeout for the users in the database (hh:mm:ss).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## RADIUS Inspect Map

The RADIUS pane lets you view previously configured RADIUS application inspection maps. A RADIUS map lets you change the default configuration values used for RADIUS application inspection. You can use a RADIUS map to protect against an overbilling attack.

### Fields

- Name—Enter the name of the inspect map, up to 40 characters in length.
- Description—Enter the description of the inspect map, up to 200 characters in length.
- RADIUS Inspect Maps—Table that lists the defined RADIUS inspect maps. The defined inspect maps are also listed in the RADIUS area of the Inspect Maps tree.
- Add—Adds the new RADIUS inspect map to the defined list in the RADIUS Inspect Maps table and to the RADIUS area of the Inspect Maps tree. To configure the new RADIUS map, select the RADIUS entry in Inspect Maps tree.
- Delete—Deletes the application inspection map selected in the RADIUS Inspect Maps table and from the RADIUS area of the Inspect Maps tree.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## RADIUS Inspect Map Host

The RADIUS Inspect Map Host Parameters pane lets you configure the host parameter settings for the inspect map.

### Fields

- Name—Shows the name of the previously configured RADIUS accounting map.
- Description—Enter the description of the RADIUS accounting map, up to 200 characters in length.
- Host Parameters—Lets you configure host parameters.
  - Host IP Address—Specify the IP address of the host that is sending the RADIUS messages.
  - Key: (optional)—Specify the key.

- Add—Adds the host entry to the Host table.
- Delete—Deletes the host entry from the Host table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## RADIUS Inspect Map Other

The RADIUS Inspect Map Other Parameters pane lets you configure additional parameter settings for the inspect map.

### Fields

- Name—Shows the name of the previously configured RADIUS accounting map.
- Description—Enter the description of the RADIUS accounting map, up to 200 characters in length.
- Other Parameters—Lets you configure additional parameters.
  - Send response to the originator of the RADIUS message—Sends a message back to the host from which the RADIUS message was sent.
  - Enforce timeout—Enables the timeout for users.  
Users Timeout—Timeout for the users in the database (hh:mm:ss).
  - Enable detection of GPRS accounting—Enables detection of GPRS accounting. This option is only available when GTP/GPRS license is enabled.
  - Validate Attribute—Attribute information.  
Attribute Number—Specify the attribute number to validate when an Accounting Start is received.  
Add—Adds the entry to the Attribute table.  
Delete—Deletes the entry from the Attribute table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |





## CHAPTER 23

# Applying AAA for Network Access

---

This chapter describes how to enable AAA (pronounced “triple A”) for network access.

For information about AAA for management access, see the [“Configuring AAA for System Administrators”](#) section on page 16-20.

This chapter includes the following sections:

- [AAA Performance, page 23-1](#)
- [Configuring Authentication for Network Access, page 23-1](#)
- [Configuring Authorization for Network Access, page 23-9](#)
- [Configuring Accounting for Network Access, page 23-15](#)
- [Using MAC Addresses to Exempt Traffic from Authentication and Authorization, page 23-16](#)

## AAA Performance

The security appliance uses “cut-through proxy” to significantly improve performance compared to a traditional proxy server. The performance of a traditional proxy server suffers because it analyzes every packet at the application layer of the OSI model. The security appliance cut-through proxy challenges a user initially at the application layer and then authenticates against standard AAA servers or the local database. After the security appliance authenticates the user, it shifts the session flow, and all traffic flows directly and quickly between the source and destination while maintaining session state information.

## Configuring Authentication for Network Access

This section includes the following topics:

- [Information About Authentication, page 23-2](#)
- [Configuring Network Access Authentication, page 23-4](#)
- [Enabling the Redirection Method of Authentication for HTTP and HTTPS, page 23-5](#)
- [Enabling Secure Authentication of Web Clients, page 23-5](#)
- [Authenticating Directly with the Security Appliance, page 23-6](#)
- [Configuring the Authentication Proxy Limit, page 23-9](#)

## Information About Authentication

The security appliance lets you configure network access authentication using AAA servers. This section includes the following topics:

- [One-Time Authentication, page 23-2](#)
- [Applications Required to Receive an Authentication Challenge, page 23-2](#)
- [Security Appliance Authentication Prompts, page 23-2](#)
- [Static PAT and HTTP, page 23-3](#)
- [Configuring Network Access Authentication, page 23-4](#)

### One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the Configuration > Firewall > Advanced > Global Timeouts pane for timeout values.) For example, if you configure the security appliance to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

### Applications Required to Receive an Authentication Challenge

Although you can configure the security appliance to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the security appliance allows other traffic requiring authentication.

The authentication ports that the security appliance supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

### Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured on the Configuration > Firewall > AAA Rules > Advanced > AAA Rules Advanced Options dialog box; see the [“Enabling the Redirection Method of Authentication for HTTP and HTTPS”](#) section on page 23-5).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured on the Configuration > Firewall > AAA Rules > Advanced > AAA Rules Advanced Options dialog box; see the [“Enabling the Redirection Method of Authentication for HTTP and HTTPS”](#) section on page 23-5).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure virtual HTTP (see the Configuration > Firewall > Advanced Options > Virtual Access pane).

**Note**

If you use HTTP authentication, by default the username and password are sent from the client to the security appliance in clear text; in addition, the username and password are sent on to the destination web server as well. See the [“Enabling Secure Authentication of Web Clients” section on page 23-5](#) for information to secure your credentials.

For FTP, a user has the option of entering the security appliance username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the security appliance password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jamiec@patm
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

## Static PAT and HTTP

For HTTP authentication, the security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the security appliance intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the security appliance intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the security appliance allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

## Configuring Network Access Authentication

To enable network access authentication, perform the following steps. For more information about authentication, see the [“Information About Authentication” section on page 23-2](#).


- 
- Step 1** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authentication Rule**.  
The Add Authentication Rule dialog box appears.
- Step 2** From the Interface drop-down list, choose the interface for applying the rule.
- Step 3** In the Action field, click one of the following, depending on the implementation:
- **Authenticate**
  - **Do not Authenticate.**
- Step 4** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the [“Configuring AAA Server Groups” section on page 14-9](#) for more information.  
  
If you chose LOCAL for the AAA server group, you can optionally add a new user by clicking **Add User**. See the [“Adding a User Account” section on page 14-17](#) for more information.
- Step 5** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 6** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 7** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 8** (Optional) In the Description field, add a description.
- Step 9** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field.  
The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
  - To make the rule inactive, uncheck **Enable Rule**.  
You may not want to remove a rule, but instead turn it off.
  - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges, page 19-15](#).
- Step 10** Click **OK**.  
The dialog box closes and the rule appears in the AAA Rules table.
- Step 11** Click **Apply**.  
The changes are saved to the running configuration.
-



## Enabling the Redirection Method of Authentication for HTTP and HTTPS

This method of authentication enables HTTP(S) listening ports to authenticate network users. When you enable a listening port, the security appliance serves an authentication page for direct connections and, by enabling redirection, for through traffic. This method also prevents the authentication credentials from continuing to the destination server. See the [“Security Appliance Authentication Prompts” section on page 23-2](#) for more information about the redirection method versus the basic method.

To enable a AAA listener, perform the following steps:

- 
- Step 1** From the Configuration > Firewall > AAA Rules pane, click **Advanced**.  
The AAA Rules Advanced Options dialog box appears.
- Step 2** Under Interactive Authentication, click **Add**.  
The Add Interactive Authentication Entry dialog box appears.
- Step 3** For the Protocol, choose either **HTTP** or **HTTPS**. You can enable both by repeating this procedure and creating two separate rules.
- Step 4** From the Interface drop-down list, choose the interface on which you want to enable the listener.
- Step 5** From the Port drop-down list, choose the port or enter a number.  
This is the port that the security appliance listens on for direct or redirected traffic; the defaults are 80 (HTTP) and 443 (HTTPS). You can use any port number and retain the same functionality, but be sure your direct authentication users know the port number; redirected traffic is sent to the correct port number automatically, but direct authenticators must specify the port number manually.
- Step 6** (Optional) Check **Redirect network users for authentication request**.  
This option redirects through traffic to an authentication web page served by the security appliance. Without this option, only traffic directed to the security appliance interface can access the authentication web pages.
-  **Note** If you enable the redirect option, you cannot also configure static PAT for the same interface where you translate the interface IP address and the same port that is used for the listener; NAT succeeds, but authentication fails.
- 
- Step 7** Click **OK**, and then click **OK** to exit the AAA Rules Advanced Options dialog box.
- Step 8** Click **Apply**.
- 

## Enabling Secure Authentication of Web Clients

If you use HTTP authentication, by default the username and password are sent from the client to the security appliance in clear text; in addition, the username and password are sent on to the destination web server as well. The security appliance provides several methods of securing HTTP authentication, including the following methods:

- Enable the redirection method of authentication for HTTP—See the [“Enabling the Redirection Method of Authentication for HTTP and HTTPS” section on page 23-5](#). This method prevents the authentication credentials from continuing to the destination server.

- Enabling Virtual HTTP—Virtual HTTP lets you authenticate separately with the security appliance and with the HTTP server. Even if the HTTP server does not need a second authentication, this feature achieves the effect of stripping the basic authentication credentials from the HTTP GET request. See the [“Authenticating HTTP\(S\) Connections with a Virtual Server”](#) section on page 23-7 for more information.
- Enabling the Exchange of Usernames and Passwords Using HTTPS—To enable the exchange of usernames and passwords between a web client and the security appliance with HTTPS, perform the following steps:
  - a. From the Configuration > Firewall > AAA Rules pane, click **Advanced**. The AAA Rules Advanced Options dialog box appears.
  - b. Under Secure HTTP, click **Enable Secure HTTP**.
  - c. Click **OK**, and then click **OK** to exit the AAA Rules Advanced Options dialog box. Click **Apply**.

This is the only method that protects credentials between the client and the security appliance, as well as between the security appliance and the destination server. You can use this method alone, or in conjunction with either of the other methods so you can maximize your security.

After enabling this feature, when a user requires authentication when using HTTP, the security appliance redirects the HTTP user to an HTTPS prompt. After you authenticate correctly, the security appliance redirects you to the original HTTP URL.

Secured web-client authentication has the following limitations:

- A maximum of 16 concurrent HTTPS authentication sessions are allowed. If all 16 HTTPS authentication processes are running, a new connection requiring authentication will not succeed.
- When the uauth timeout is set to unlimited, HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the uauth timeout to 1 second (see the Configuration > Firewall > Advanced > Global Timeouts pane). However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.
- Because HTTPS authentication occurs on the SSL port 443, users must not configure an Access Rule to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port.

## Authenticating Directly with the Security Appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can authenticate with the security appliance directly using HTTP, HTTPS, or Telnet.

- [Authenticating Telnet Connections with a Virtual Server, page 23-7](#)
- [Authenticating HTTP\(S\) Connections with a Virtual Server, page 23-7](#)

## Authenticating Telnet Connections with a Virtual Server

Although you can configure network access authentication for any protocol or service (see the [“Configuring Authentication for Network Access” section on page 23-1](#)), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the security appliance, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate according to the [“Configuring Authentication for Network Access” section on page 23-1](#).

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the Access Rule applied to the source interface. Moreover, you must add a static NAT rule for the virtual Telnet IP address, even if NAT is not required. An identity NAT rule is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an Access Rule to an inside interface, be sure to allow access to the virtual Telnet address. A static NAT rule is not required.

To logout from the security appliance, reconnect to the virtual Telnet IP address; you are prompted to log out.

To enable direct authentication using Telnet, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Configuration > Firewall > Advanced > Virtual Access > Virtual Telnet Server area, check the <b>Enable</b> check box.                                                                                                                                                                                                                                                                                          |
| <b>Step 2</b> | In the Virtual Telnet Server field, add the IP address of the virtual Telnet server.<br><br>Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses accessing an outside server, and you want to provide outside access to the virtual HTTP server, you can use one of the global NAT addresses for the virtual HTTP server address. |
| <b>Step 3</b> | Click <b>Apply</b> .<br><br>The virtual server is added and the changes are saved to the running configuration.                                                                                                                                                                                                                                                                                                         |
- 

## Authenticating HTTP(S) Connections with a Virtual Server

When you use HTTP authentication on the security appliance (see the [“Configuring Authentication for Network Access” section on page 23-1](#)), the security appliance uses basic HTTP authentication by default. You can change the authentication method so that the security appliance redirects HTTP connections to web pages generated by the security appliance itself using the [“Configuring HTTP Redirect” section on page 6-4](#).

However, if you continue to use basic HTTP authentication, then you might need the virtual HTTP server when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the security appliance, then virtual HTTP lets you authenticate separately with the security appliance (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This feature redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

For inbound users (from lower security to higher security), you must also include the virtual HTTP address as a destination interface in the Access Rule applied to the source interface. Moreover, you must add a static NAT rule for the virtual HTTP IP address, even if NAT is not required. An identity NAT rule is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an Access Rule to an inside interface, be sure to allow access to the virtual HTTP address. A static NAT rule is not required.



#### Note

Do not set the uauth timeout duration to 0 seconds when using virtual HTTP, because this setting prevents HTTP connections to the real web server. See the [“Configuring Global Timeouts” section on page 27-23](#).

You can authenticate directly with the security appliance at the following URLs when you enable AAA for the interface:

```
http://interface_ip[:port]/netaccess/connstatus.html
https://interface_ip[:port]/netaccess/connstatus.html
```

To allow users to authenticate with the security appliance virtual server separately from the HTTP server, perform the following steps:

- Step 1** From the Configuration > Firewall > Advanced > Virtual Access > Virtual HTTP Server area, check the **Enable** check box.
- Step 2** In the Virtual HTTP Server field, add the IP address of the virtual HTTP server.  
Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses accessing an outside server, and you want to provide outside access to the virtual HTTP server, you can use one of the global NAT addresses for the virtual HTTP server address.
- Step 3** (Optional) If you are using text-based browsers, where redirection does not happen automatically, check the **Display redirection warning** check box. This enables an alert to notify users when the HTTP connection is being redirected.
- Step 4** Click **Apply**.  
The virtual server is added and the changes are saved to the running configuration.

## Configuring the Authentication Proxy Limit

You can manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user.

To set the proxy limit, perform the following steps:

- 
- |               |                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Configuration > Firewall > AAA Rules pane, click <b>Advanced</b> .<br>The AAA Rules Advanced Options dialog box appears. |
| <b>Step 2</b> | In the Proxy Limit area, check <b>Enable Proxy Limit</b> .                                                                        |
| <b>Step 3</b> | In the Proxy Limit field, enter the number of concurrent proxy connections allowed per user, from 1 to 128.                       |
| <b>Step 4</b> | Click <b>OK</b> , and then click <b>Apply</b> .                                                                                   |
- 

## Configuring Authorization for Network Access

After a user authenticates for a given connection, the security appliance can use authorization to further control traffic from the user.

This section includes the following topics:

- [Configuring TACACS+ Authorization, page 23-9](#)
- [Configuring RADIUS Authorization, page 23-10](#)

## Configuring TACACS+ Authorization

You can configure the security appliance to perform network access authorization with TACACS+.

Authentication and authorization rules are independent; however, any unauthenticated traffic matched by an authorization rule will be denied. For authorization to succeed:

1. A user must first authenticate with the security appliance.  
Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session hasn't expired, authorization can occur even if the traffic is not matched by an authentication rule.
2. After a user authenticates, the security appliance checks the authorization rules for matching traffic.
3. If the traffic matches the authorization rule, the security appliance sends the username to the TACACS+ server.
4. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile.
5. The security appliance enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

To configure TACACS+ authorization, perform the following steps:

- 
- Step 1** Enable authentication. For more information, see the [“Configuring Network Access Authentication” section on page 23-4](#). If you have already enabled authentication, continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Authorization Rule**.  
The Add Authorization Rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface for applying the rule.
- Step 4** In the Action field, click one of the following, depending on the implementation:
- **Authorize**
  - **Do not Authorize.**
- Step 5** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the [“Configuring AAA Server Groups” section on page 14-9](#) for more information.  
Only TACACS+ servers are supported.
- Step 6** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 7** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 8** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 9** (Optional) In the Description field, add a description.
- Step 10** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field.  
The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
  - To make the rule inactive, uncheck **Enable Rule**.  
You may not want to remove a rule, but instead turn it off.
  - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges, page 19-15](#).
- Step 11** Click **OK**.  
The dialog box closes and the rule appears in the AAA Rules table.
- Step 12** Click **Apply**.  
The changes are saved to the running configuration.
- 

## Configuring RADIUS Authorization

When authentication succeeds, the RADIUS protocol returns user authorizations in the access-accept message sent by a RADIUS server. For more information about configuring authentication, see the [“Configuring Authentication for Network Access” section on page 23-1](#).

When you configure the security appliance to authenticate users for network access, you are also implicitly enabling RADIUS authorizations; therefore, this section contains no information about configuring RADIUS authorization on the security appliance. It does provide information about how the security appliance handles access list information received from RADIUS servers.

You can configure a RADIUS server to download an access list to the security appliance or an access list name at the time of authentication. The user is authorized to do only what is permitted in the user-specific access list.

**Note**

If you have enabled the Per User Override Setting (see the Configuration > Firewall > Access Rules > Advanced > Access Rules Advanced Options dialog box), be aware of the following effects of this feature on authorization by user-specific access lists:

- Without the per-user-override feature, traffic for a user session must be permitted by both the interface access list and the user-specific access list.
- With the per-user-override feature, the user-specific access list determines what is permitted.

This section includes the following topics:

- [Configuring a RADIUS Server to Send Downloadable Access Control Lists, page 23-11](#)
- [Configuring a RADIUS Server to Download Per-User Access Control List Names, page 23-15](#)

## Configuring a RADIUS Server to Send Downloadable Access Control Lists

This section describes how to configure Cisco Secure ACS or a third-party RADIUS server, and includes the following topics:

- [About the Downloadable Access List Feature and Cisco Secure ACS, page 23-11](#)
- [Configuring Cisco Secure ACS for Downloadable Access Lists, page 23-13](#)
- [Configuring Any RADIUS Server for Downloadable Access Lists, page 23-14](#)
- [Converting Wildcard Netmask Expressions in Downloadable Access Lists, page 23-15](#)

### About the Downloadable Access List Feature and Cisco Secure ACS

Downloadable access lists is the most scalable means of using Cisco Secure ACS to provide the appropriate access lists for each user. It provides the following capabilities:

- Unlimited access list size—Downloadable access lists are sent using as many RADIUS packets as required to transport the full access list from Cisco Secure ACS to the security appliance.
- Simplified and centralized management of access lists—Downloadable access lists enable you to write a set of access lists once and apply it to many user or group profiles and distribute it to many security appliances.

This approach is most useful when you have very large access list sets that you want to apply to more than one Cisco Secure ACS user or group; however, its ability to simplify Cisco Secure ACS user and group management makes it useful for access lists of any size.

The security appliance receives downloadable access lists from Cisco Secure ACS using the following process:

1. The security appliance sends a RADIUS authentication request packet for the user session.

2. If Cisco Secure ACS successfully authenticates the user, Cisco Secure ACS returns a RADIUS access-accept message that contains the internal name of the applicable downloadable access list. The Cisco IOS cisco-av-pair RADIUS VSA (vendor 9, attribute 1) contains the following attribute-value pair to identify the downloadable access list set:

```
ACS:CiscoSecure-Defined-ACL=acl-set-name
```

where *acl-set-name* is the internal name of the downloadable access list, which is a combination of the name assigned to the access list by the Cisco Secure ACS administrator and the date and time that the access list was last modified.

3. The security appliance examines the name of the downloadable access list and determines if it has previously received the named downloadable access list.
  - If the security appliance has previously received the named downloadable access list, communication with Cisco Secure ACS is complete and the security appliance applies the access list to the user session. Because the name of the downloadable access list includes the date and time it was last modified, matching the name sent by Cisco Secure ACS to the name of an access list previously downloaded means that the security appliance has the most recent version of the downloadable access list.
  - If the security appliance has not previously received the named downloadable access list, it may have an out-of-date version of the access list or it may not have downloaded any version of the access list. In either case, the security appliance issues a RADIUS authentication request using the downloadable access list name as the username in the RADIUS request and a null password attribute. In a cisco-av-pair RADIUS VSA, the request also includes the following attribute-value pairs:

```
AAA:service=ip-admission
AAA:event=acl-download
```

In addition, the security appliance signs the request with the Message-Authenticator attribute (IETF RADIUS attribute 80).

4. Upon receipt of a RADIUS authentication request that has a username attribute containing the name of a downloadable access list, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. If the Message-Authenticator attribute is missing or incorrect, Cisco Secure ACS ignores the request. The presence of the Message-Authenticator attribute prevents malicious use of a downloadable access list name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions, available at <http://www.ietf.org>.
5. If the access list required is less than approximately 4 KB in length, Cisco Secure ACS responds with an access-accept message containing the access list. The largest access list that can fit in a single access-accept message is slightly less than 4 KB because some of the message must be other required attributes.

Cisco Secure ACS sends the downloadable access list in a cisco-av-pair RADIUS VSA. The access list is formatted as a series of attribute-value pairs that each contain an ACE and are numbered serially:

```
ip:inacl#1=ACE-1
ip:inacl#2=ACE-2
.
.
.
ip:inacl#n=ACE-n
```

An example of an attribute-value pair follows:

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```



6. If the access list required is more than approximately 4 KB in length, Cisco Secure ACS responds with an access-challenge message that contains a portion of the access list, formatted as described above, and an State attribute (IETF RADIUS attribute 24), which contains control data used by Cisco Secure ACS to track the progress of the download. Cisco Secure ACS fits as many complete attribute-value pairs into the cisco-av-pair RADIUS VSA as it can without exceeding the maximum RADIUS message size.

The security appliance stores the portion of the access list received and responds with another access-request message containing the same attributes as the first request for the downloadable access list plus a copy of the State attribute received in the access-challenge message.

This repeats until Cisco Secure ACS sends the last of the access list in an access-accept message.

### Configuring Cisco Secure ACS for Downloadable Access Lists

You can configure downloadable access lists on Cisco Secure ACS as a shared profile component and then assign the access list to a group or to an individual user.

The access list definition consists of one or more security appliance commands that are similar to the extended **access-list** command, except without the following prefix:

**access-list** *acl\_name* **extended**

The following example is a downloadable access list definition on Cisco Secure ACS version 3.3:

```
+-----+
| Shared profile Components |
| |
| Downloadable IP ACLs Content |
| |
| Name: acs_ten_acl |
| |
| ACL Definitions |
| |
| permit tcp any host 10.0.0.254 |
| permit udp any host 10.0.0.254 |
| permit icmp any host 10.0.0.254 |
| permit tcp any host 10.0.0.253 |
| permit udp any host 10.0.0.253 |
| permit icmp any host 10.0.0.253 |
| permit tcp any host 10.0.0.252 |
| permit udp any host 10.0.0.252 |
| permit icmp any host 10.0.0.252 |
| permit ip any any |
+-----+
```

For more information about creating downloadable access lists and associating them with users, see the user guide for your version of Cisco Secure ACS.

On the security appliance, the downloaded access list has the following name:

#ACSACL#-ip-acl\_name-number

The *acl\_name* argument is the name that is defined on Cisco Secure ACS (acs\_ten\_acl in the preceding example), and *number* is a unique version ID generated by Cisco Secure ACS.

The downloaded access list on the security appliance consists of the following lines:

```
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
```

```

access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit ip any any

```

## Configuring Any RADIUS Server for Downloadable Access Lists

You can configure any RADIUS server that supports Cisco IOS RADIUS VSAs to send user-specific access lists to the security appliance in a Cisco IOS RADIUS cisco-av-pair VSA (vendor 9, attribute 1).

In the cisco-av-pair VSA, configure one or more ACEs that are similar to the **access-list extended** command, except that you replace the following command prefix:

**access-list** *acl\_name* **extended**

with the following text:

**ip:inacl#nnn=**

The *nnn* argument is a number in the range from 0 to 999999999 that identifies the order of the command statement to be configured on the security appliance. If this parameter is omitted, the sequence value is 0, and the order of the ACEs inside the cisco-av-pair RADIUS VSA is used.

The following example is an access list definition as it should be configured for a cisco-av-pair VSA on a RADIUS server:

```

ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0

```

For information about making unique per user the access lists that are sent in the cisco-av-pair attribute, see the documentation for your RADIUS server.

On the security appliance, the downloaded access list name has the following format:

*AAA-user-username*

The *username* argument is the name of the user that is being authenticated.

The downloaded access list on the security appliance consists of the following lines. Notice the order based on the numbers identified on the RADIUS server.

```

access-list AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list AAA-user-bcham34-79AD4A08 deny tcp any any
access-list AAA-user-bcham34-79AD4A08 deny udp any any

```

Downloaded access lists have two spaces between the word “access-list” and the name. These spaces serve to differentiate a downloaded access list from a local access list. In this example, “79AD4A08” is a hash value generated by the security appliance to help determine when access list definitions have changed on the RADIUS server.

## Converting Wildcard Netmask Expressions in Downloadable Access Lists

If a RADIUS server provides downloadable access lists to Cisco VPN 3000 series concentrators as well as to the security appliance, you may need the security appliance to convert wildcard netmask expressions to standard netmask expressions. This is because Cisco VPN 3000 series concentrators support wildcard netmask expressions but the security appliance only supports standard netmask expressions. Configuring the security appliance to convert wildcard netmask expressions helps minimize the effects of these differences upon how you configure downloadable access lists on your RADIUS servers. Translation of wildcard netmask expressions means that downloadable access lists written for Cisco VPN 3000 series concentrators can be used by the security appliance without altering the configuration of the downloadable access lists on the RADIUS server.

You configure access list netmask conversion on a per-server basis when you add a server to a server group, on the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area. See the [“Adding a Server to a Group”](#) section on page 14-10.

## Configuring a RADIUS Server to Download Per-User Access Control List Names

To download a name for an access list that you already created on the security appliance (at the CLI) from the RADIUS server when a user authenticates, configure the IETF RADIUS filter-id attribute (attribute number 11) as follows:

```
filter-id=acl_name
```



### Note

In Cisco Secure ACS, the value for filter-id attributes are specified in boxes in the HTML interface, omitting **filter-id=** and entering only *acl\_name*.

For information about making unique per user the filter-id attribute value, see the documentation for your RADIUS server.

See the *Cisco Security Appliance Command Line Configuration Guide* to create an access list on the security appliance.

# Configuring Accounting for Network Access

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

To configure accounting, perform the following steps:

- Step 1** If you want the security appliance to provide accounting data per user, you must enable authentication. For more information, see the [“Configuring Network Access Authentication”](#) section on page 23-4. If you want the security appliance to provide accounting data per IP address, enabling authentication is not necessary and you can continue to the next step.
- Step 2** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add Accounting Rule**. The Add Accounting Rule dialog box appears.

- Step 3** From the Interface drop-down list, choose the interface for applying the rule.
- Step 4** In the Action field, click one of the following, depending on the implementation:
- **Account**
  - **Do not Account.**
- Step 5** From the AAA Server Group drop-down list, choose a server group. To add a AAA server to the server group, click **Add Server**. See the [“Configuring AAA Server Groups” section on page 14-9](#) for more information.
- Step 6** In the Source field, add the source IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 7** In the Destination field, enter the destination IP address, or click the ellipsis (...) to choose an IP address already defined in ASDM.
- Step 8** In the Service field, enter an IP service name or number for the destination service, or click ellipsis (...) button to choose a service.
- Step 9** (Optional) In the Description field, add a description.
- Step 10** (Optional) Click **More Options** to do any of the following:
- To specify a source service for TCP or UDP, enter a TCP or UDP service in the Source Service field. The destination service and source service must be the same. Copy and paste the destination Service field to the Source Service field.
  - To make the rule inactive, uncheck **Enable Rule**.  
You may not want to remove a rule, but instead turn it off.
  - To set a time range for the rule, from the Time Range drop-down list, choose an existing time range. To add a new time range, click the ellipsis (...). For more information, see [Configuring Time Ranges, page 19-15](#).
- Step 11** Click **OK**.  
The dialog box closes and the rule appears in the AAA Rules table.
- Step 12** Click **Apply**.  
The changes are saved to the running configuration.
- 

## Using MAC Addresses to Exempt Traffic from Authentication and Authorization

The security appliance can exempt from authentication and authorization any traffic from specific MAC addresses.

For example, if the security appliance authenticates TCP traffic originating on a particular network but you want to allow unauthenticated TCP connections from a specific server, you would use a MAC exempt rule to exempt from authentication and authorization any traffic from the server specified by the rule. This feature is particularly useful to exempt devices such as IP phones that cannot respond to authentication prompts.

The order of entries matters, because the packet uses the first entry it matches, as opposed to a best match scenario. If you have a permit entry, and you want to deny an address that is allowed by the permit entry, be sure to enter the deny entry before the permit entry.

To use MAC addresses to exempt traffic from authentication and authorization, perform the following steps:

**Step 13** From the Configuration > Firewall > AAA Rules pane, choose **Add > Add MAC Exempt Rule**.

The Add MAC Exempt Rule dialog box appears.

**Step 14** From the Action drop-down list, click one of the following, depending on the implementation:

- **MAC Exempt**
- **No MAC Exempt**

The MAC Exempt option allows traffic from the MAC address without having to authenticate or authorize. The No MAC Exempt option specifies a MAC address that is not exempt from authentication or authorization. You might need to add a deny entry if you permit a range of MAC addresses using a MAC address mask such as ffff.fff.0000, and you want to force a MAC address in that range to be authenticated and authorized.

**Step 15** In the MAC Address field, specify the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn.

**Step 16** In the MAC Mask field, specify the portion of the MAC address that should be used for matching. For example, ffff.fff.fff matches the MAC address exactly. ffff.fff.0000 matches only the first 8 digits.

**Step 17** Click **OK**.

The dialog box closes and the rule appears in the AAA Rules table.

**Step 18** Click **Apply**.

The changes are saved to the running configuration.

---





# CHAPTER 24

## Configuring Application Layer Protocol Inspection

---

This chapter describes how to configure application layer protocol inspection. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the security appliance to do a deep packet inspection instead of passing the packet through the fast path. As a result, inspection engines can affect overall throughput.

Several common inspection engines are enabled on the security appliance by default, but you might need to enable others depending on your network. This chapter includes the following sections:

- [Inspection Engine Overview, page 24-2](#)
  - [When to Use Application Protocol Inspection, page 24-2](#)
  - [Inspection Limitations, page 24-3](#)
  - [Default Inspection Policy, page 24-3](#)
- [Configuring Application Inspection, page 24-4](#)
- [CTIQBE Inspection, page 24-5](#)
- [DCERPC Inspection, page 24-6](#)
- [DNS Inspection, page 24-6](#)
- [ESMTP Inspection, page 24-8](#)
- [FTP Inspection, page 24-8](#)
- [GTP Inspection, page 24-10](#)
- [H.323 Inspection, page 24-11](#)
- [HTTP Inspection, page 24-13](#)
- [Instant Messaging Inspection, page 24-14](#)
- [ICMP Inspection, page 24-14](#)
- [ICMP Error Inspection, page 24-14](#)
- [ILS Inspection, page 24-14](#)
- [MGCP Inspection, page 24-15](#)
- [MMP Inspection, page 24-17](#)
- [NetBIOS Inspection, page 24-18](#)
- [PPTP Inspection, page 24-19](#)

- [RADIUS Accounting Inspection, page 24-19](#)
- [RSH Inspection, page 24-19](#)
- [RTSP Inspection, page 24-19](#)
- [SIP Inspection, page 24-21](#)
- [Skinny \(SCCP\) Inspection, page 24-22](#)
- [SMTP and Extended SMTP Inspection, page 24-24](#)
- [SNMP Inspection, page 24-25](#)
- [SQL\\*Net Inspection, page 24-25](#)
- [Sun RPC Inspection, page 24-26](#)
- [TFTP Inspection, page 24-28](#)
- [XDMCP Inspection, page 24-28](#)
- [Service Policy Field Descriptions, page 24-28](#)
- [Class Map Field Descriptions, page 24-39](#)
- [Inspect Map Field Descriptions, page 24-59](#)

## Inspection Engine Overview

This section includes the following topics:

- [When to Use Application Protocol Inspection, page 24-2](#)
- [Inspection Limitations, page 24-3](#)
- [Default Inspection Policy, page 24-3](#)

## When to Use Application Protocol Inspection

When a user establishes a connection, the security appliance checks the packet against access lists, creates an address translation, and creates an entry for the session in the fast path, so that further packets can bypass time-consuming checks. However, the fast path relies on predictable port numbers and does not perform address translations inside a packet.

Many protocols open secondary TCP or UDP ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers.

Other applications embed an IP address in the packet that needs to match the source address that is normally translated when it goes through the security appliance.

If you use applications like these, then you need to enable application inspection.

When you enable application inspection for a service that embeds IP addresses, the security appliance translates embedded addresses and updates any checksum or other fields that are affected by the translation.

When you enable application inspection for a service that uses dynamically assigned ports, the security appliance monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.



## Inspection Limitations

See the following limitations for application protocol inspection:

- State information for multimedia sessions that require inspection are not passed over the state link for stateful failover. The exception is GTP, which is replicated over the state link.
- Some inspection engines do not support PAT, NAT, outside NAT, or NAT between same security interfaces. See [“Default Inspection Policy”](#) for more information about NAT support.

## Default Inspection Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy, so if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one.

[Table 24-1](#) lists all inspections supported, the default ports used in the default class map, and the inspection engines that are on by default, shown in bold. This table also notes any NAT limitations.

**Table 24-1 Supported Application Inspection Engines**

| Application <sup>1</sup>   | Default Port                                   | NAT Limitations                                               | Standards <sup>2</sup>                         | Comments                                                                                                                                                              |
|----------------------------|------------------------------------------------|---------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CTIQBE                     | TCP/2748                                       | —                                                             | —                                              | —                                                                                                                                                                     |
| DNS over UDP               | UDP/53                                         | No NAT support is available for name resolution through WINS. | RFC 1123                                       | No PTR records are changed.                                                                                                                                           |
| FTP                        | TCP/21                                         | —                                                             | RFC 959                                        | —                                                                                                                                                                     |
| GTP                        | UDP/3386<br>UDP/2123                           | —                                                             | —                                              | Requires a special license.                                                                                                                                           |
| <b>H.323 H.225 and RAS</b> | TCP/1720<br>UDP/1718<br>UDP (RAS)<br>1718-1719 | No NAT on same security interfaces.<br>No static PAT.         | ITU-T H.323,<br>H.245, H225.0,<br>Q.931, Q.932 | —                                                                                                                                                                     |
| HTTP                       | TCP/80                                         | —                                                             | RFC 2616                                       | Beware of MTU limitations stripping ActiveX and Java. If the MTU is too small to allow the Java or ActiveX tag to be included in one packet, stripping may not occur. |
| ICMP                       | —                                              | —                                                             | —                                              | All ICMP traffic is matched in the default class map.                                                                                                                 |
| ICMP ERROR                 | —                                              | —                                                             | —                                              | All ICMP traffic is matched in the default class map.                                                                                                                 |
| ILS (LDAP)                 | TCP/389                                        | No PAT.                                                       | —                                              | —                                                                                                                                                                     |
| MGCP                       | UDP/2427,<br>2727                              | —                                                             | RFC 2705bis-05                                 | —                                                                                                                                                                     |

**Table 24-1** Supported Application Inspection Engines (continued)

| Application <sup>1</sup>           | Default Port                | NAT Limitations                                        | Standards <sup>2</sup>           | Comments                                                                                                                                                                                    |
|------------------------------------|-----------------------------|--------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NetBIOS Name Server over IP</b> | UDP/137, 138 (Source ports) | —                                                      | —                                | NetBIOS is supported by performing NAT of the packets for NBNS UDP port 137 and NBDS UDP port 138.                                                                                          |
| PPTP                               | TCP/1723                    | —                                                      | RFC 2637                         | —                                                                                                                                                                                           |
| RADIUS Accounting                  | 1646                        | —                                                      | RFC 2865                         | —                                                                                                                                                                                           |
| <b>RSH</b>                         | TCP/514                     | No PAT                                                 | Berkeley UNIX                    | —                                                                                                                                                                                           |
| RTSP                               | TCP/554                     | No PAT.<br>No outside NAT.                             | RFC 2326, 2327, 1889             | No handling for HTTP cloaking.                                                                                                                                                              |
| <b>SIP</b>                         | TCP/5060<br>UDP/5060        | No outside NAT.<br>No NAT on same security interfaces. | RFC 2543                         | —                                                                                                                                                                                           |
| <b>SKINNY (SCCP)</b>               | TCP/2000                    | No outside NAT.<br>No NAT on same security interfaces. | —                                | Does not handle TFTP uploaded Cisco IP Phone configurations under certain circumstances.                                                                                                    |
| <b>SMTP and ESMTP</b>              | TCP/25                      | —                                                      | RFC 821, 1123                    | —                                                                                                                                                                                           |
| SNMP                               | UDP/161, 162                | No NAT or PAT.                                         | RFC 1155, 1157, 1212, 1213, 1215 | v.2 RFC 1902-1908; v.3 RFC 2570-2580.                                                                                                                                                       |
| <b>SQL*Net</b>                     | TCP/1521                    | —                                                      | —                                | v.1 and v.2.                                                                                                                                                                                |
| <b>Sun RPC over UDP and TCP</b>    | UDP/111                     | No NAT or PAT.                                         | —                                | The default rule includes UDP port 111; if you want to enable Sun RPC inspection for TCP port 111, you need to create a new rule that matches TCP port 111 and performs Sun RPC inspection. |
| TFTP                               | UDP/69                      | —                                                      | RFC 1350                         | Payload IP addresses are not translated.                                                                                                                                                    |
| <b>XDCMP</b>                       | UDP/177                     | No NAT or PAT.                                         | —                                | —                                                                                                                                                                                           |

1. Inspection engines that are enabled by default for the default port are in bold.
2. The security appliance is in compliance with these standards, but it does not enforce compliance on packets being inspected. For example, FTP commands are supposed to be in a particular order, but the security appliance does not enforce the order.

## Configuring Application Inspection

This feature uses Security Policy Rules. Service policies provide a consistent and flexible way to configure security appliance features. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications. See [Chapter 22, “Configuring Service Policy Rules,”](#) for more information.

Inspection is enabled by default for some applications. See the [“Default Inspection Policy”](#) section for more information. Use this section to modify your inspection policy.

To configure application inspection, perform the following steps:

- 
- Step 1** Click **Configuration > Firewall > Service Policy Rules**.
- Step 2** Add or edit a service policy rule according to the [“Adding a Service Policy Rule for Through Traffic” section on page 22-6](#).
- If you want to match non-standard ports, then create a new rule for the non-standard ports. See the [“Default Inspection Policy” section on page 24-3](#) for the standard ports for each inspection engine. You can combine multiple rules in the same service policy if desired, so you can create one rule to match certain traffic, and another to match different traffic. However, if traffic matches a rule that contains an inspection action, and then matches another rule that also has an inspection action, only the first matching rule is used.
- Step 3** On the Edit Service Policy Rule > Rule Actions dialog box, click the **Protocol Inspection** tab.
- For a new rule, the dialog box is called Add Service Policy Rule Wizard - Rule Actions.
- Step 4** Check each inspection type that you want to apply.
- Step 5** (Optional) Some inspection engines let you control additional parameters when you apply the inspection to the traffic. Click **Configure** for each inspection type to configure an inspect map.
- You can either choose an existing map, or create a new one. You can predefine inspect maps from the Configuration > Firewall > Objects > Inspect Maps pane. See the [“Inspect Map Field Descriptions” section on page 24-59](#) for detailed information of each inspect map type.
- Step 6** You can configure other features for this rule if desired using the other Rule Actions tabs.
- Step 7** Click **OK** (or **Finish** from the wizard).
- 

## CTIQBE Inspection

This section describes CTIQBE application inspection. This section includes the following topics:

- [CTIQBE Inspection Overview, page 24-5](#)
- [Limitations and Restrictions, page 24-5](#)

## CTIQBE Inspection Overview

CTIQBE protocol inspection supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the security appliance.

TAPI and JTAPI are used by many Cisco VoIP applications. CTIQBE is used by Cisco TSP to communicate with Cisco CallManager.

## Limitations and Restrictions

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations with the **alias** command.
- Stateful failover of CTIQBE calls is not supported.

- Entering the **debug ctique** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the security appliance, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the security appliance, calls between these two phones fails.
- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the same port of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

## DCERPC Inspection

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The security appliance allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.

DCERPC inspect maps inspect for native TCP communication between the EPM and client on well known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have user configurable timeouts.

## DNS Inspection

This section describes DNS application inspection. This section includes the following topics:

- [How DNS Application Inspection Works, page 24-6](#)
- [How DNS Rewrite Works, page 24-7](#)

## How DNS Application Inspection Works

The security appliance tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the security appliance. The security appliance also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

When DNS inspection is enabled, which is the default, the security appliance performs the following additional tasks:

- Translates the DNS record based on the configuration completed using NAT rules. Translation only applies to the A-record in the DNS reply; therefore, DNS Rewrite does not affect reverse lookups, which request the PTR record.



**Note** DNS Rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 65535 bytes). The security appliance performs reassembly as needed to verify that the packet length is less than the maximum length configured. The security appliance drops the packet if it exceeds the maximum length.
- Enforces a domain-name length of 255 bytes and a label length of 63 bytes.
- Verifies the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message.
- Checks to see if a compression pointer loop exists.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app\_id*, and the idle timer for each *app\_id* runs independently.

Because the *app\_id* expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, if you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

## How DNS Rewrite Works

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

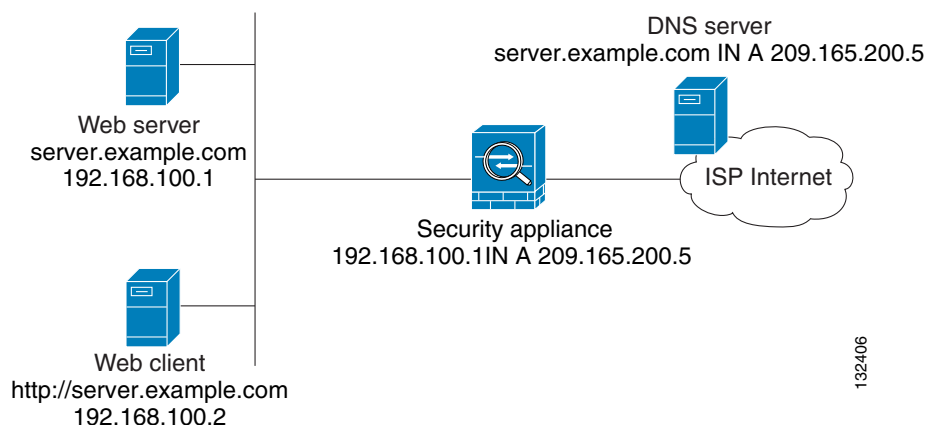
If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

As long as DNS inspection remains enabled, you can configure DNS rewrite using a NAT rule.

DNS Rewrite performs two functions:

- Translating a public address (the routable or “mapped” address) in a DNS reply to a private address (the “real” address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

In [Figure 24-1](#), the DNS server resides on the external (ISP) network. The real address of the server (192.168.100.1) has been mapped using a static NAT rule to the ISP-assigned address (209.165.200.5). When a web client on the inside interface attempts to access the web server with the URL `http://server.example.com`, the host running the web client sends a DNS request to the DNS server to resolve the IP address of the web server. The security appliance translates the non-routable source address in the IP header and forwards the request to the ISP network on its outside interface. When the DNS reply is returned, the security appliance applies address translation not only to the destination address, but also to the embedded IP address of the web server, which is contained in the A-record in the DNS reply. As a result, the web client on the inside network gets the correct address for connecting to the web server on the inside network.

**Figure 24-1** Translating the Address in a DNS Reply (DNS Rewrite)

DNS rewrite also works if the client making the DNS request is on a DMZ network and the DNS server is on an inside interface.

## ESMTP Inspection

ESMTP inspection detects attacks, including spam, phishing, malformed message attacks, buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detect several attacks, block senders/receivers, and block mail relay.

## FTP Inspection

This section describes the FTP inspection engine. This section includes the following topics:

- [FTP Inspection Overview, page 24-8](#)
- [Using Strict FTP, page 24-9](#)
- [Verifying and Monitoring FTP Inspection, page 24-10](#)

## FTP Inspection Overview

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address

FTP application inspection prepares secondary channels for FTP data transfer. Ports for these channels are negotiated through PORT or PASV commands. The channels are allocated in response to a file upload, a file download, or a directory listing event.

**Note**

If you disable FTP inspection engines, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

## Using Strict FTP

Using strict FTP increases the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. To enable strict FTP, click the **Configure** button next to FTP on the Configuration > Firewall > Service Policy Rules > Edit Service Policy Rule > Rule Actions > Protocol Inspection tab.

**Note**

To specify FTP commands that are not permitted to pass through the security appliance, create an FTP inspect map according to the [“FTP Class Map” section on page 24-43](#).

After you enable the Strict option on an interface, FTP inspection enforces the following behavior:

- An FTP command must be acknowledged before the security appliance allows a new command.
- The security appliance drops connections that send embedded commands.
- The 227 and PORT commands are checked to ensure they do not appear in an error string.

**Caution**

Using the strict option may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

If the strict option is enabled, each FTP command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the PORT and PASV reply command is checked to see if it is five. If it is not five, then the PORT command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the FTP command to see if it ends with <CR><LF> characters, as required by the RFC. If it does not, the connection is closed.
- Size of RETR and STOR commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The PORT command should always be sent from the client. The TCP connection is denied if a PORT command is sent from the server.
- Reply spoofing—PASV reply command (227) should always be sent from the server. The TCP connection is denied if a PASV reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing—The security appliance closes the connection if it detects TCP stream editing.
- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. As port numbers in the range from 1 to 1024 are reserved for well-known connections, if the negotiated port falls in this range, then the TCP connection is freed.
- Command pipelining—The number of characters present after the port numbers in the PORT and PASV reply command is cross checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.

- The security appliance replaces the FTP server response to the SYST command with a series of Xs. to prevent the server from revealing its system type to FTP clients. To override this default behavior, use the Low setting in the FTP map.

## Verifying and Monitoring FTP Inspection

FTP application inspection generates the following log messages:

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

## GTP Inspection

**Note**

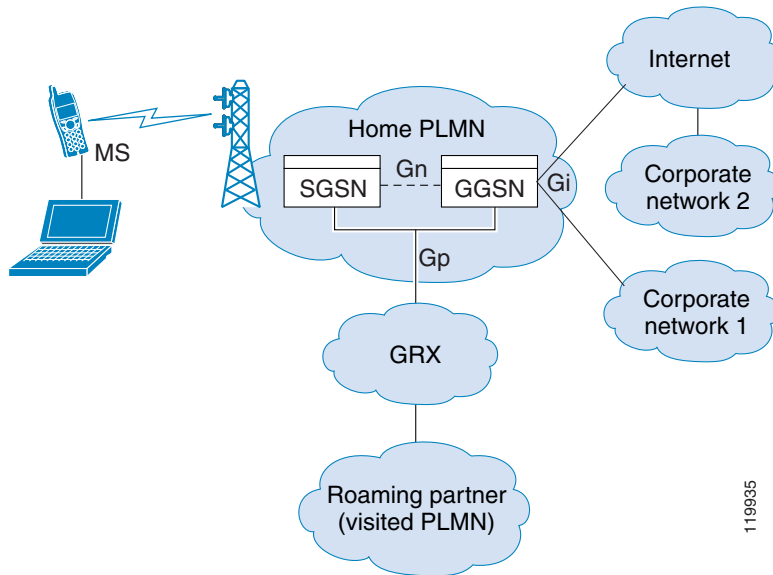
---

GTP inspection requires a special license.

---

GPRS provides uninterrupted connectivity for mobile subscribers between GSM networks and corporate networks or the Internet. The GGSN is the interface between the GPRS wireless data network and other networks. The SGSN performs mobility, data session management, and data compression (See [Figure 24-2](#)).



**Figure 24-2 GPRS Tunneling Protocol**

The UMTS is the commercial convergence of fixed-line telephony, mobile, Internet and computer technology. UTRAN is the networking protocol used for implementing wireless networks in this system. GTP allows multi-protocol packets to be tunneled through a UMTS/GPRS backbone between a GGSN, an SGSN and the UTRAN.

GTP does not include any inherent security or encryption of user data, but using GTP with the security appliance helps protect your network against these risks.

The SGSN is logically connected to a GGSN using GTP. GTP allows multiprotocol packets to be tunneled through the GPRS backbone between GSNs. GTP provides a tunnel control and management protocol that allows the SGSN to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP uses a tunneling mechanism to provide a service for carrying user data packets.

**Note**

When using GTP with failover, if a GTP connection is established and the active unit fails before data is transmitted over the tunnel, the GTP data connection (with a “j” flag set) is not replicated to the standby unit. This occurs because the active unit does not replicate embryonic connections to the standby unit.

## H.323 Inspection

This section describes the H.323 application inspection. This section includes the following topics:

- [H.323 Inspection Overview, page 24-12](#)
- [How H.323 Works, page 24-12](#)
- [Limitations and Restrictions, page 24-13](#)

## H.323 Inspection Overview

H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The security appliance supports H.323 through Version 4, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the security appliance.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.
- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

## How H.323 Works

The H.323 collection of protocols collectively may use up to two TCP connection and four to six UDP connections. FastConnect uses only one TCP connection, and RAS uses a single UDP connection for registration, admissions, and status.

An H.323 client may initially establish a TCP connection to an H.323 server using TCP port 1720 to request Q.931 call setup. As part of the call setup process, the H.323 terminal supplies a port number to the client to use for an H.245 TCP connection. In environments where H.323 gatekeeper is in use, the initial packet is transmitted using UDP.

H.323 inspection monitors the Q.931 TCP connection to determine the H.245 port number. If the H.323 terminals are not using FastConnect, the security appliance dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP data streams. H.323 inspection inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. RTP uses the negotiated port number, while RTCP uses the next higher port number.

The H.323 control channel handles H.225 and H.245 and H.323 RAS. H.323 inspection uses the following ports.

- 1718—Gate Keeper Discovery UDP port
- 1719—RAS UDP port
- 1720—TCP Control Port

You must permit traffic for the well-known H.323 port 1720 for the H.225 call signaling; however, the H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the security appliance opens an H.225 connection based on inspection of the ACF message.

After inspecting the H.225 messages, the security appliance opens the H.245 channel and then inspects traffic sent over the H.245 channel as well. All H.245 messages passing through the security appliance undergo H.245 application inspection, which translates embedded IP addresses and opens the media channels negotiated in H.245 messages.

The H.323 ITU standard requires that a TPKT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as H.225 and H.245 messages, the security appliance must remember the TPKT length to process and decode the messages properly. For each connection, the security appliance keeps a record that contains the TPKT length for the next expected message.

If the security appliance needs to perform NAT on IP addresses in messages, it changes the checksum, the UUIE length, and the TPKT, if it is included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, the security appliance proxy ACKs that TPKT and appends a new TPKT to the H.245 message with the new length.

**Note**

The security appliance does not support TCP options in the Proxy ACK for the TPKT.

Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and times out with the H.323 timeout as configured on the Configuration > Firewall > Advanced > Global Timeouts pane.

## Limitations and Restrictions

The following are some of the known issues and limitations when using H.323 application inspection:

- Static PAT may not properly translate IP addresses embedded in optional fields within H.323 messages. If you experience this kind of problem, do not use static PAT with H.323.
- H.323 application inspection is not supported with NAT between same-security-level interfaces.
- When a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the security appliance.
- If you configure a network static address where the network static address is the same as a third-party netmask and address, then any outbound H.323 connection fails.

## HTTP Inspection

Use the HTTP inspection engine to protect against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions:

- Enhanced HTTP inspection
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

The latter two features are configured in conjunction with Filter rules.

The enhanced HTTP inspection feature, which is also known as an application firewall and is available when you configure an HTTP inspect map (see the [“HTTP Class Map” section on page 24-48](#)), can help prevent attackers from using HTTP messages for circumventing network security policy. It verifies the following for all HTTP messages:

- Conformance to RFC 2616
- Use of RFC-defined methods only.
- Compliance with the additional criteria.

# Instant Messaging Inspection

The IM inspect engine lets you apply fine grained controls on the IM application to control the network usage and stop leakage of confidential data, propagation of worms, and other threats to the corporate network.

## ICMP Inspection

The ICMP inspection engine allows ICMP traffic to have a “session” so it can be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the security appliance in an access list. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct.

## ICMP Error Inspection

When this feature is enabled, the security appliance creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The security appliance overwrites the packet with the translated IP addresses.

When disabled, the security appliance does not create translation sessions for intermediate nodes that generate ICMP error messages. ICMP error messages generated by the intermediate nodes between the inside host and the security appliance reach the outside host without consuming any additional NAT resource. This is undesirable when an outside host uses the traceroute command to trace the hops to the destination on the inside of the security appliance. When the security appliance does not translate the intermediate hops, all the intermediate hops appear with the mapped destination IP address.

The ICMP payload is scanned to retrieve the five-tuple from the original packet. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. The ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the mapped IP is changed to the real IP (Destination Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet mapped IP is changed to the real IP
  - Original packet mapped port is changed to the real Port
  - Original packet IP checksum is recalculated

## ILS Inspection

The ILS inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The security appliance supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the security appliance border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the Configuration > Firewall > Advanced > Global Timeouts pane.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment

ILS inspection has the following limitations:

- Referral requests and responses are not supported
- Users in multiple directories are not unified
- Single users having multiple identities in multiple directories cannot be recognized by NAT

**Note**

Because H225 call signalling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP option on the Configuration > Firewall > Advanced > Global Timeouts pane. By default, this interval is set at 60 minutes.

## MGCP Inspection

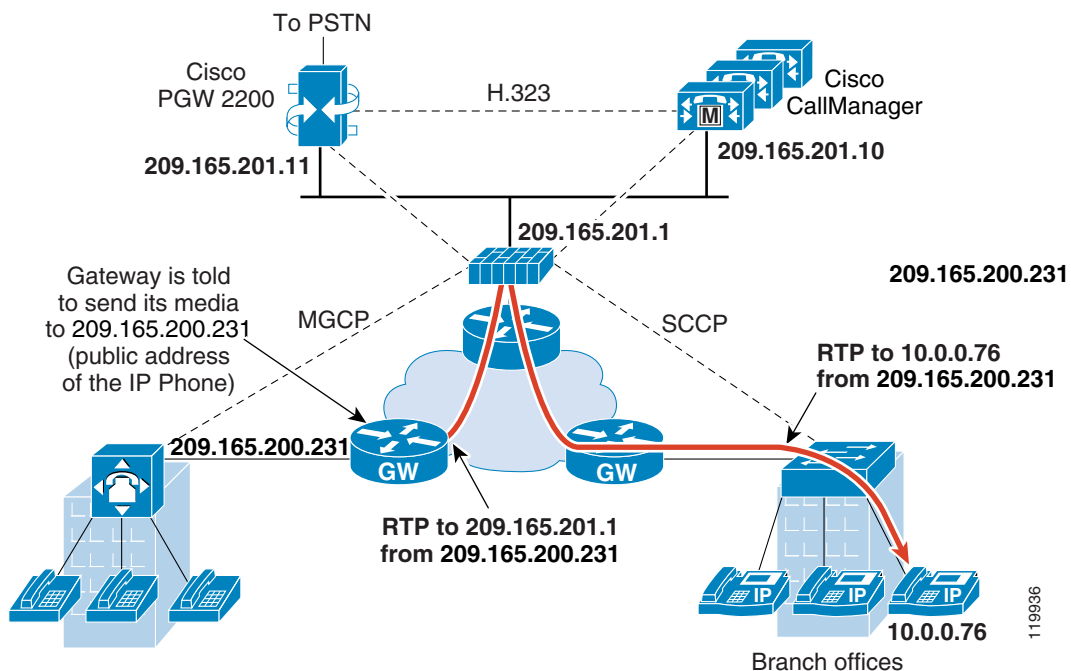
MGCP is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over

the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses. Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, broad-band wireless devices.
- Business gateways, that provide a traditional digital PBX interface or an integrated soft PBX interface to a Voice over IP network.

MGCP messages are transmitted over UDP. A response is sent back to the source address (IP address and UDP port number) of the command, but the response may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response. [Figure 24-3](#) illustrates how NAT can be used with MGCP.

**Figure 24-3** Using NAT with MGCP



MGCP endpoints are physical or virtual sources and destinations for data. Media gateways contain endpoints on which the call agent can create, modify and delete connections to establish and control media sessions with other multimedia endpoints. Also, the call agent can instruct the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the call agent.

MGCP transactions are composed of a command and a mandatory response. There are eight types of commands:

- CreateConnection
- ModifyConnection

- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

The first four commands are sent by the call agent to the gateway. The Notify command is sent by the gateway to the call agent. The gateway may also send a DeleteConnection. The registration of the MGCP gateway with the call agent is achieved by the RestartInProgress command. The AuditEndpoint and the AuditConnection commands are sent by the call agent to the gateway.

All commands are composed of a Command header, optionally followed by a session description. All responses are composed of a Response header, optionally followed by a session description.

- The port on which the gateway receives commands from the call agent. Gateways usually listen to UDP port 2427.
- The port on which the call agent receives commands from the gateway. Call agents usually listen to UDP port 2727.

**Note**

MGCP inspection does not support the use of different IP addresses for MGCP signaling and RTP data. A common and recommended practice is to send RTP data from a resilient IP address, such as a loopback or virtual IP address; however, the security appliance requires the RTP data to come from the same address as MGCP signalling.

## MMP Inspection

The security appliance includes an inspection engine to validate the CUMA Mobile Multiplexing Protocol (MMP).

For information about setting up the TLS Proxy for the Mobility Advantage feature, see [TLS Proxy, page 19-17](#).

MMP is a data transport protocol for transmitting data entities between CUMA clients and servers. MMP must be run on top of a connection-oriented protocol (the underlying transport) and is intended to be run on top of a secure transport protocol such as TLS. The Orative Markup Language (OML) protocol is intended to be run on top of MMP for the purposes of data synchronization, as well as the HTTP protocol for uploading and downloading large files.

The TCP/TLS default port is 5443. There are no embedded NAT or secondary connections.

CUMA client and server communications can be proxied via TLS, which decrypts the data, passes it to the inspect MMP module, and re-encrypt the data before forwarding it to the endpoint. The inspect MMP module verifies the integrity of the MMP headers and passes the OML/HTTP to an appropriate handler. The security appliance takes the following actions on the MMP headers and data:

- Verifies that client MMP headers are well-formed. Upon detection of a malformed header, the TCP session is terminated.
- Verifies that client to server MMP header lengths are not exceeded. If an MMP header length is exceeded (4096), then the TCP session is terminated.

- Verifies that client to server MMP content lengths are not exceeded. If an entity content length is exceeded (4096), the TCP session is terminated.

**Note**

4096 is the value currently used in MMP implementations.

Since MMP headers and entities can be split across packets, the security appliance buffers data to ensure consistent inspection. The SAPI (stream API) handles data buffering for pending inspection opportunities. MMP header text is treated as case insensitive and a space is present between header text and values. Reclaiming of MMP state is performed by monitoring the state of the TCP connection. Timeouts for these connections follow existing configurable values via the **timeout** command.

MMP inspection is disabled by default. When enabled, MMP inspection operates on TCP destination and source port 5443.

## Configuring MMP Inspection for a TLS Proxy

Use the Add Service Policy Rule Wizard - Rule Actions dialog box to configure MMP protocol inspection.

This wizard is available from the Configuration > Firewall > Service Policy Rules > Add > Add Service Policy Rule Wizard - Rule Actions dialog box.

- 
- Step 1** Open the Add Service Policy Rule Wizard by selecting Configuration > Firewall > Service Policy Rules > Add. Perform the steps to complete the Service Policy, Traffic Classification Criteria, and Traffic Match - Destination Port pages of the wizard. See [Adding a Service Policy Rule for Through Traffic, page 22-6](#).
- The Add Service Policy Rule Wizard - Rule Actions dialog box opens.
- Step 2** Check the MMP check box.
- Step 3** Click **Configure** beside to the MMP check box. The Configure TLS Proxy dialog box opens.
- Step 4** Perform one of the following:
- Select the TLS Proxy for which you are enabling MMP protocol inspection.
- Or
- Click **Manage** to create a new TLS Proxy Instance. The Configure TLS Proxy dialog box opens. See [Configure TLS Proxy Pane, page 19-19](#).
- Step 5** Click **OK**.
- Step 6** Click **Finish**.
- 

## NetBIOS Inspection

NetBIOS inspection is enabled by default. The NetBios inspection engine translates IP addresses in the NetBios name service (NBNS) packets according to the security appliance NAT configuration.



## PPTP Inspection

PPTP is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE [RFC 2637] when negotiated over the PPTP TCP control channel. Port Address Translation is *not* performed for the unmodified version of GRE [RFC 1701, RFC 1702].

Specifically, the security appliance inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network.

## RADIUS Accounting Inspection

See the [“Select RADIUS Accounting Map” section on page 22-14](#) for information about RADIUS accounting inspection.

## RSH Inspection

RSH inspection is enabled by default. The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

## RTSP Inspection

This section describes RTSP application inspection. This section includes the following topics:

- [RTSP Inspection Overview, page 24-20](#)
- [Using RealPlayer, page 24-20](#)
- [Restrictions and Limitations, page 24-20](#)

## RTSP Inspection Overview

The RTSP inspection engine lets the security appliance pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

**Note**

For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The security appliance only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that is used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The security appliance parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the security appliance and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the security appliance does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the security appliance keeps state and remembers the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

RTSP inspection does not support PAT or dual-NAT. Also, the security appliance cannot recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.

## Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the security appliance, add an Access Rule from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the security appliance, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the security appliance, add an **inspect rtsp port** command.

## Restrictions and Limitations

The following restrictions apply to RTSP inspection:

- The security appliance does not support multicast RTSP or RTSP messages over UDP.
- PAT is not supported.
- The security appliance does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The security appliance cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and security appliance cannot perform NAT on fragmented packets.

- With Cisco IP/TV, the number of translates the security appliance performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.

## SIP Inspection

This section describes SIP application inspection. This section includes the following topics:

- [SIP Inspection Overview, page 24-21](#)
- [SIP Instant Messaging, page 24-21](#)

### SIP Inspection Overview

SIP, as defined by the IETF, enables call handling sessions, particularly two-party audio conferences, or “calls.” SIP works with SDP for call signalling. SDP specifies the ports for the media stream. Using SIP, the security appliance can support any SIP VoIP gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

The following limitations and restrictions apply when using PAT with SIP:

- If a remote endpoint tries to register with a SIP proxy on a network protected by the security appliance, the registration fails under very specific conditions, as follows:
  - PAT is configured for the remote endpoint.
  - The SIP registrar server is on the outside network.
  - The port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.
- If a SIP device transmits a packet in which the SDP portion has an IP address in the owner/creator field (o=) that is different than the IP address in the connection field (c=), the IP address in the o= field may not be properly translated. This is due to a limitation in the SIP protocol, which does not provide a port value in the o= field.

### SIP Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. SIP supports the Chat feature on Windows XP using Windows Messenger RTC Client version 4.7.0105 only. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes that time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.

**Note**

Only the Chat feature is currently supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

SIP inspection translates the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL\_ID/FROM/TO from the SIP payload. These indices identify the call, the source, and the destination. This database contains the media addresses and media ports found in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. The security appliance opens RTP/RTCP connections between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message; however, subsequent messages may not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be translated.

As a call is set up, the SIP session is in the “transient” state until the media address and media port is received from the called endpoint in a Response message indicating the RTP port the called endpoint listens on. If there is a failure to receive the response messages within one minute, the signaling connection is torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection remains until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface does not traverse the security appliance, unless the security appliance configuration specifically allows it.

## Skinny (SCCP) Inspection

This section describes SCCP application inspection. This section includes the following topics:

- [SCCP Inspection Overview, page 24-23](#)
- [Supporting Cisco IP Phones, page 24-23](#)
- [Restrictions and Limitations, page 24-24](#)

**Note**

For specific information about setting up the Phone Proxy on the security appliance, which is part of the Cisco Unified Communications architecture and supports IP Phone deployment, see [Phone Proxy, page 19-24](#).

## SCCP Inspection Overview

Skinny (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323 compliant terminals. Application layer functions in the security appliance recognize SCCP Version 3.3. There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2. The security appliance supports all versions through Version 3.3.2.

**Note**

For specific information about setting up the Phone Proxy on the security appliance, which is part of the Cisco Unified Communications architecture and supports IP Phone deployment, see [Phone Proxy, page 19-24](#).

The security appliance supports PAT and NAT for SCCP. PAT is necessary if you have more IP phones than global IP addresses for the IP phones to use. By supporting NAT and PAT of SCCP Signaling packets, Skinny application inspection ensures that all SCCP signalling and media packets can traverse the security appliance.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The security appliance also supports DHCP options 150 and 66, which it accomplishes by sending the location of a TFTP server to Cisco IP Phones and other DHCP clients. Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

## Supporting Cisco IP Phones

**Note**

For specific information about setting up the Phone Proxy on the security appliance, which is part of the Cisco Unified Communications architecture and supports IP Phone deployment, see [Phone Proxy, page 19-24](#).

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be **static** as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An static identity entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an access list to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an identity static entry. When using NAT, an identity static entry maps to the same IP address. When using PAT, it maps to the same IP address and port.

When the Cisco IP Phones are on a *higher* security interface compared to the TFTP server and Cisco CallManager, no access list or static entry is required to allow the Cisco IP Phones to initiate the connection.

## Restrictions and Limitations



### Note

For specific information about setting up the Phone Proxy on the security appliance, which is part of the Cisco Unified Communications architecture and supports IP Phone deployment, see [Phone Proxy, page 19-24](#).

The following are limitations that apply to the current version of PAT and NAT support for SCCP:

- PAT does not work with configurations containing the **alias** command.
- Outside NAT or PAT is *not* supported.

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones fail because the security appliance currently does not support NAT or PAT for the file content transferred over TFTP. Although the security appliance supports NAT of TFTP messages and opens a pinhole for the TFTP file, the security appliance cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone configuration files that are transferred by TFTP during phone registration.



### Note

The security appliance supports stateful failover of SCCP calls except for calls that are in the middle of call setup.

## SMTP and Extended SMTP Inspection

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the security appliance and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar in most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

Extended SMTP application inspection adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the security appliance supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTTLS, ONEX, VERB, CHUNKING, and private extensions are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “O” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP may hang if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human-readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character (|) is deleted (changed to a blank space) and "<" , ">" are only allowed if they are used to define a mail address (">" must be preceded by "<").
- Unexpected transition by the SMTP server.
- For unknown commands, the security appliance changes all the characters in the packet to X. In this case, the server generates an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

## SNMP Inspection

SNMP application inspection lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The security appliance can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map.

## SQL\*Net Inspection

SQL\*Net inspection is enabled by default.

The SQL\*Net protocol consists of different packet types that the security appliance handles to make the data stream appear consistent to the Oracle applications on either side of the security appliance.

The default port assignment for SQL\*Net is 1521. This is the value used by Oracle for SQL\*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL\*Net inspection to a range of port numbers.

The security appliance translates all addresses and looks in the packets for all embedded ports to open for SQL\*Net Version 1.

For SQL\*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL\*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL\*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the security appliance, a flag will be set in the connection data structure to expect the Data or Redirect message that follows to be translated and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL\*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL\*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be translated and port connections will be opened.

## Sun RPC Inspection

This section describes Sun RPC application inspection. This section includes the following topics:

- [Sun RPC Inspection Overview, page 24-26](#)
- [SUNRPC Server, page 24-26](#)

## Sun RPC Inspection Overview

The Sun RPC inspection engine enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access an Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbind, on the well-known port of 111.

The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the security appliance intercepts this packet and opens both embryonic TCP and UDP connections on that port.



### Note

NAT or PAT of Sun RPC payload information is not supported.

## SUNRPC Server

The Configuration > Firewall > Advanced > **SUNRPC Server** pane shows which SunRPC services can traverse the security appliance and their specific timeout, on a per server basis.

### Fields

- **Interface**—Displays the interface on which the SunRPC server resides.



- **IP address**—Displays the IP address of the SunRPC server.
- **Mask**—Displays the subnet mask of the IP Address of the SunRPC server.
- **Service ID**—Displays the SunRPC program number, or service ID, allowed to traverse the security appliance.
- **Protocol**—Displays the SunRPC transport protocol (TCP or UDP).
- **Port**—Displays the SunRPC protocol port range.
- **Timeout**—Displays the idle time after which the access for the SunRPC service traffic is closed.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SUNRPC Service

The Configuration > Firewall > Advanced > **SUNRPC Server** > **Add/Edit SUNRPC Service** dialog box lets you specify what SunRPC services are allowed to traverse the security appliance and their specific timeout, on a per-server basis.

### Fields

- **Interface Name**—Specifies the interface on which the SunRPC server resides.
- **Protocol**—Specifies the SunRPC transport protocol (TCP or UDP).
- **IP address**—Specifies the IP address of the SunRPC server.
- **Port**—Specifies the SunRPC protocol port range.
- **Mask**—Specifies the subnet mask of the IP Address of the SunRPC server.
- **Timeout**—Specifies the idle time after which the access for the SunRPC service traffic is closed. Format is HH:MM:SS.
- **Service ID**—Specifies the SunRPC program number, or service ID, allowed to traverse the security appliance.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## TFTP Inspection

TFTP inspection is enabled by default.

TFTP, described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

## XDMCP Inspection

XDMCP inspection is enabled by default; however, the XDMCP inspection engine is dependent upon proper configuration of the **established** command.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the security appliance must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the security appliance. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000  $n$ . Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where  $n$  is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the security appliance can NAT if needed. XDCMP inspection does not support PAT.

## Service Policy Field Descriptions

This section lists the field descriptions for each protocol inspection dialog box, and includes the following topics:

- [Rule Actions > Protocol Inspection Tab, page 24-29](#)
- [Select DCERPC Map, page 24-31](#)
- [Select DNS Map, page 24-31](#)
- [Select ESMTTP Map, page 24-32](#)
- [Select FTP Map, page 24-32](#)
- [Select GTP Map, page 24-33](#)

- [Select H.323 Map, page 24-33](#)
- [Select HTTP Map, page 24-34](#)
- [Select IM Map, page 24-34](#)
- [Select IPSec-Pass-Thru Map, page 24-35](#)
- [Select MGCP Map, page 24-35](#)
- [Select NETBIOS Map, page 24-36](#)
- [Select RTSP Map, page 24-36](#)
- [Select SCCP \(Skinny\) Map, page 24-37](#)
- [Select SIP Map, page 24-37](#)
- [Select SNMP Map, page 24-38](#)

## Rule Actions > Protocol Inspection Tab

### Fields

- **CTIQBE**—Enables application inspection for the CTIQBE protocol.
- **DCERPC**—Enables application inspection for the DCERPC protocol.
  - **Configure**—Displays the **Select DCERPC Map** dialog box, which lets you select a map name to use for this protocol.
- **DNS**—Enables application inspection for the DNS protocol.
  - **Configure**—Displays the **Select DNS Map** dialog box, which lets you select a map name to use for this protocol.
- **ESMTP**—Enables application inspection for the ESMTP protocol.
  - **Configure**—Displays the **Select ESMTP Map** dialog box, which lets you select a map name to use for this protocol.
- **FTP**—Enables application inspection for the FTP protocol.
  - **Configure**—Displays the **Select FTP Map** dialog box, which lets you select a map name to use for this protocol.
- **GTP**—Enables application inspection for the GTP protocol.
  - **Configure**—Displays the **Select GTP Map** dialog box, which lets you select a map name to use for this protocol.



### Note

GTP inspection is not available without a special license.

- **H323 H225**—Enables application inspection for the H323 H225 protocol.
  - **Configure**—Displays the **Select H323 H225 Map** dialog box, which lets you select a map name to use for this protocol.
- **H323 RAS**—Enables application inspection for the H323 RAS protocol.
  - **Configure**—Displays the **Select H323 RAS Map** dialog box, which lets you select a map name to use for this protocol.
- **HTTP**—Enables application inspection for the HTTP protocol.

- **Configure**—Displays the **Select HTTP Map** dialog box, which lets you select a map name to use for this protocol.
- **ICMP**—Enables application inspection for the ICMP protocol.
- **ICMP Error**—Enables application inspection for the ICMP Error protocol.
- **ILS**—Enables application inspection for the ILS protocol.
- **IM**—Enables application inspection for the IM protocol.
  - **Configure**—Displays the **Select IM Map** dialog box, which lets you select a map name to use for this protocol.
- **IPSec-Pass-Thru**—Enables application inspection for the IPSec protocol.
  - **Configure**—Displays the **Select IPSec Map** dialog box, which lets you select a map name to use for this protocol.
- **MGCP**—Enables application inspection for the MGCP protocol.
  - **Configure**—Displays the **Select MGCP Map** dialog box, which lets you select a map name to use for this protocol.
- **NETBIOS**—Enables application inspection for the NetBIOS protocol.
  - **Configure**—Displays the **Select NETBIOS Map** dialog box, which lets you select a map name to use for this protocol.
- **PPTP**—Enables application inspection for the PPTP protocol.
- **RSH**—Enables application inspection for the RSH protocol.
- **RTSP**—Enables application inspection for the RTSP protocol.
- **SCCP SKINNY**—Enables application inspection for the Skinny protocol.
  - **Configure**—Displays the **Select SCCP (Skinny) Map** dialog box, which lets you select a map name to use for this protocol.
- **SIP**—Enables application inspection for the SIP protocol.
  - **Configure**—Displays the **Select SIP Map** dialog box, which lets you select a map name to use for this protocol.
- **SNMP**—Enables application inspection for the SNMP protocol.
  - **Configure**—Displays the **Select SNMP Map** dialog box, which lets you select a map name to use for this protocol.
- **SQLNET**—Enables application inspection for the SQLNET protocol.
- **SUNRPC**—Enables application inspection for the SunRPC protocol.
- **TFTP**—Enables application inspection for the TFTP protocol.
- **XDMCP**—Enables application inspection for the XDMCP protocol.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

[Inspect Map Field Descriptions, page 24-59](#)

**Inspect** command pages for each protocol in the *Cisco Security Appliance Command Reference*.

## Select DCERPC Map

The **Select DCERPC Map** dialog box lets you select or create a new **DCERPC** map. A **DCERPC** map lets you change the configuration values used for **DCERPC** application inspection. The **Select DCERPC Map** table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default DCERPC inspection map**—Specifies to use the default DCERPC map.
- **Select a DCERPC map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select DNS Map

The **Select DNS Map** dialog box lets you select or create a new **DNS** map. A **DNS** map lets you change the configuration values used for **DNS** application inspection. The **Select DNS Map** table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default DNS inspection map**—Specifies to use the default **DNS** map.
- **Select a DNS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select ESMTP Map

The **Select ESMTP Map** dialog box lets you select or create a new **ESMTP** map. An **ESMTP** map lets you change the configuration values used for **ESMTP** application inspection. The **Select ESMTP Map** table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default ESMTP inspection map**—Specifies to use the default **ESMTP** map.
- **Select an ESMTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select FTP Map

The **Select FTP Map** dialog box lets you enable strict FTP application inspection, select an FTP map, or create a new FTP map. An FTP map lets you change the configuration values used for FTP application inspection. The **Select FTP Map** table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **FTP Strict (prevent web browsers from sending embedded commands in FTP requests)**—Enables strict FTP application inspection, which causes the security appliance to drop the connection when an embedded command is included in an FTP request.
- **Use the default FTP inspection map**—Specifies to use the default FTP map.
- **Select an FTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select GTP Map

The **Select GTP Map** dialog box lets you select or create a new GTP map. A GTP map lets you change the configuration values used for GTP application inspection. The Select GTP Map table provides a list of previously configured maps that you can select for application inspection.



**Note** GTP inspection requires a special license. If you try to enable GTP application inspection on a security appliance without the required license, the security appliance displays an error message.

**Fields**

- **Use the default GTP inspection map**—Specifies to use the default GTP map.
- **Select an GTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select H.323 Map

The **Select H.323 Map** dialog box lets you select or create a new **H.323** map. An **H.323** map lets you change the configuration values used for **H.323** application inspection. The Select **H.323** Map table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default H.323 inspection map**—Specifies to use the default **H.323** map.
- **Select an H.323 map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select HTTP Map

The **Select HTTP Map** dialog box lets you select or create a new HTTP map. An HTTP map lets you change the configuration values used for HTTP application inspection. The Select HTTP Map table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default HTTP inspection map**—Specifies to use the default HTTP map.
- **Select an HTTP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select IM Map

The **Select IM Map** dialog box lets you select or create a new **IM** map. An **IM** map lets you change the configuration values used for **IM** application inspection. The Select **IM** Map table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select IPSec-Pass-Thru Map

The **Select IPSec-Pass-Thru** dialog box lets you select or create a new **IPSec** map. An **IPSec** map lets you change the configuration values used for **IPSec** application inspection. The **Select IPSec Map** table provides a list of previously configured maps that you can select for application inspection.

### Fields

- **Use the default IPSec inspection map**—Specifies to use the default **IPSec** map.
- **Select an IPSec map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select MGCP Map

The **Select MGCP Map** dialog box lets you select or create a new **MGCP** map. An **MGCP** map lets you change the configuration values used for **MGCP** application inspection. The **Select MGCP Map** table provides a list of previously configured maps that you can select for application inspection.

### Fields

- **Use the default MGCP inspection map**—Specifies to use the default **MGCP** map.
- **Select an MGCP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select NETBIOS Map

The **Select NETBIOS Map** dialog box lets you select or create a new **NetBIOS** map. A **NetBIOS** map lets you change the configuration values used for **NetBIOS** application inspection. The **Select NetBIOS Map** table provides a list of previously configured maps that you can select for application inspection.

### Fields

- **Use the default IM inspection map**—Specifies to use the default **NetBIOS** map.
- **Select a NetBIOS map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select RTSP Map

The **Select RTSP Map** dialog box lets you select or create a new **RTSP** map. An **RTSP** map lets you change the configuration values used for **RTSP** application inspection. The **Select RTSP Map** table provides a list of previously configured maps that you can select for application inspection.

### Fields

- **Use the default RTSP inspection map**—Specifies to use the default **RTSP** inspection map.
- **Select a RTSP inspect map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select SCCP (Skinny) Map

The **Select SCCP (Skinny) Map** dialog box lets you select or create a new **SCCP (Skinny)** map. An **SCCP (Skinny)** map lets you change the configuration values used for **SCCP (Skinny)** application inspection. The **Select SCCP (Skinny) Map** table provides a list of previously configured maps that you can select for application inspection.

### Fields

- **Use the default SCCP (Skinny) inspection map**—Specifies to use the default **SCCP (Skinny)** map.
- **Select an SCCP (Skinny) map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.
- **Encrypted Traffic Inspection**—Lets you specify TLS proxy settings for the inspect map.
  - **Do not inspect Encrypted Traffic**—Disables the inspection of Skinny application inspection.
  - **Use Phone Proxy to enable inspection of encrypted traffic**—Uses the Phone Proxy configured on the security appliance to inspect Skinny application traffic. See [Phone Proxy, page 19-24](#).
  - **Use TLS Proxy to enable inspection of encrypted traffic**—Specifies to use Transaction Layer Security Proxy to enable inspection of encrypted traffic.

TLS Proxy Name:—Name of existing TLS Proxy.

New—Opens the Add TLS Proxy dialog box to add a TLS Proxy.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select SIP Map

The **Select SIP Map** dialog box lets you select or create a new **SIP** map. A **SIP** map lets you change the configuration values used for **SIP** application inspection. The **Select SIP Map** table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default SIP inspection map**—Specifies to use the default **SIP** map.
- **Select a SIP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.
- **TLS Proxy**—Lets you specify TLS proxy settings for the inspect map.
  - **Use TLS Proxy to enable inspection of encrypted traffic**—Specifies to use Transaction Layer Security Proxy to enable inspection of encrypted traffic.
  - TLS Proxy Name:**—Name of existing TLS Proxy.
  - New**—Opens the Add TLS Proxy dialog box to add a TLS Proxy.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Select SNMP Map

The **Select SNMP Map** dialog box lets you select or create a new SNMP map. An SNMP map lets you change the configuration values used for SNMP application inspection. The Select SNMP Map table provides a list of previously configured maps that you can select for application inspection.

**Fields**

- **Use the default SNMP inspection map**—Specifies to use the default **SNMP** map.
- **Select an SNMP map for fine control over inspection**—Lets you select a defined application inspection map or add a new one.
- **Add**—Opens the Add Policy Map dialog box for the inspection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# Class Map Field Descriptions

An inspection class map matches application traffic with criteria specific to the application, such as a URL string. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

This section describes how to configure inspection class maps, and includes the following topics:

- [DNS Class Map, page 24-39](#)
- [FTP Class Map, page 24-43](#)
- [H.323 Class Map, page 24-46](#)
- [HTTP Class Map, page 24-48](#)
- [IM Class Map, page 24-53](#)
- [SIP Class Map, page 24-56](#)

## DNS Class Map

The DNS Class Map panel lets you configure DNS class maps for DNS inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- Name—Shows the DNS class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the DNS class map.
  - Value—Shows the value to match in the DNS class map.
- Description—Shows the description of the class map.
- Add—Adds match conditions for the DNS class map.
- Edit—Edits match conditions for the DNS class map.
- Delete—Deletes match conditions for the DNS class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# Add/Edit DNS Traffic Class Map

The Add/Edit DNS Traffic Class Map dialog box lets you define a DNS class map.

## Fields

- Name—Enter the name of the DNS class map, up to 40 characters in length.
- Description—Enter the description of the DNS class map.
- Add—Adds a DNS class map.
- Edit—Edits a DNS class map.
- Delete—Deletes a DNS class map.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

# Add/Edit DNS Match Criterion

The Add/Edit DNS Match Criterion dialog box lets you define the match criterion and value for the DNS class map.

## Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.  
  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of DNS traffic to match.
  - Header Flag—Match a DNS flag in the header.
  - Type—Match a DNS query or resource record type.
  - Class—Match a DNS query or resource record class.
  - Question—Match a DNS question.
  - Resource Record—Match a DNS resource record.
  - Domain Name—Match a domain name from a DNS query or resource record.
- Header Flag Criterion Values—Specifies the value details for the DNS header flag match.
  - Match Option—Specifies either an exact match or match all bits (bit mask match).
  - Match Value—Specifies to match either the header flag name or the header flag value.  
  
Header Flag Name—Lets you select one or more header flag names to match, including AA (authoritative answer), QR (query), RA (recursion available), RD (recursion denied), TC (truncation) flag bits.

- Header Flag Value—Lets you enter an arbitrary 16-bit value in hex to match.
- Type Criterion Values—Specifies the value details for the DNS type match.
  - DNS Type Field Name—Lists the DNS types to select.
    - A—IPv4 address
    - NS—Authoritative name server
    - CNAME—Canonical name
    - SOA—Start of a zone of authority
    - TSIG—Transaction signature
    - IXFR—Incremental (zone) transfer
    - AXFR—Full (zone) transfer
  - DNS Type Field Value—Specifies to match either a DNS type field value or a DNS type field range.
    - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
    - Range—Lets you enter a range match. Both values between 0 and 65535.
- Class Criterion Values—Specifies the value details for the DNS class match.
  - DNS Class Field Name—Specifies to match on internet, the DNS class field name.
  - DNS Class Field Value—Specifies to match either a DNS class field value or a DNS class field range.
    - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
    - Range—Lets you enter a range match. Both values between 0 and 65535.
- Question Criterion Values—Specifies to match on the DNS question section.
- Resource Record Criterion Values—Specifies to match on the DNS resource record section.
  - Resource Record—Lists the sections to match.
    - Additional—DNS additional resource record
    - Answer—DNS answer resource record
    - Authority—DNS authority resource record
- Domain Name Criterion Values—Specifies to match on the DNS domain name.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Manage Regular Expressions

The Manage Regular Expressions dialog box lets you configure [Regular Expressions](#) for use in pattern matching. Regular expressions that start with “\_default” are default regular expressions and cannot be modified or deleted.

### Fields

- Name—Shows the regular expression names.
- Value—Shows the regular expression definitions.
- Add—Adds a regular expression.
- Edit—Edits a regular expression.
- Delete—Deletes a regular expression.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Manage Regular Expression Class Maps

The Manage Regular Expression Class Maps dialog box lets you configure regular expression class maps. See [Regular Expressions](#) for more information.

### Fields

- Name—Shows the regular expression class map name.
- Match Conditions—Shows the match type and regular expressions in the class map.
  - Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.
  - Regular Expression—Lists the regular expressions included in each class map.
- Description—Shows the description of the class map.



- Add—Adds a regular expression class map.
- Edit—Edits a regular expression class map.
- Delete—Deletes a regular expression class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## FTP Class Map

The FTP Class Map panel lets you configure FTP class maps for FTP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- Name—Shows the FTP class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the FTP class map.
  - Value—Shows the value to match in the FTP class map.
- Description—Shows the description of the class map.
- Add—Adds an FTP class map.
- Edit—Edits an FTP class map.
- Delete—Deletes an FTP class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit FTP Traffic Class Map

The Add/Edit FTP Traffic Class Map dialog box lets you define a FTP class map.

### Fields

- Name—Enter the name of the FTP class map, up to 40 characters in length.
- Description—Enter the description of the FTP class map.
- Add—Adds an FTP class map.
- Edit—Edits an FTP class map.
- Delete—Deletes an FTP class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit FTP Match Criterion

The Add/Edit FTP Match Criterion dialog box lets you define the match criterion and value for the FTP class map.

### Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of FTP traffic to match.
  - Request-Command—Match an FTP request command.
  - File Name—Match a filename for FTP transfer.
  - File Type—Match a file type for FTP transfer.
  - Server—Match an FTP server.
  - User Name—Match an FTP user.
- Request-Command Criterion Values—Specifies the value details for the FTP request command match.
  - Request Command—Lets you select one or more request commands to match.  
APPE—Append to a file.  
CDUP—Change to the parent of the current directory.  
DELE—Delete a file at the server site.

GET—FTP client command for the retr (retrieve a file) command.

HELP—Help information from the server.

MKD—Create a directory.

PUT—FTP client command for the stor (store a file) command.

RMD—Remove a directory.

RNFR—Rename from.

RNTO—Rename to.

SITE—Specify a server specific command.

STOU—Store a file with a unique name.

- File Name Criterion Values—Specifies to match on the FTP transfer filename.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- File Type Criterion Values—Specifies to match on the FTP transfer file type.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Server Criterion Values—Specifies to match on the FTP server.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- User Name Criterion Values—Specifies to match on the FTP user.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## H.323 Class Map

The H.323 Class Map panel lets you configure H.323 class maps for H.323 inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- Name—Shows the H.323 class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the H.323 class map.
  - Value—Shows the value to match in the H.323 class map.
- Description—Shows the description of the class map.
- Add—Adds an H.323 class map.
- Edit—Edits an H.323 class map.
- Delete—Deletes an H.323 class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit H.323 Traffic Class Map

The Add/Edit H.323 Traffic Class Map dialog box lets you define a H.323 class map.

### Fields

- Name—Enter the name of the H.323 class map, up to 40 characters in length.
- Description—Enter the description of the H.323 class map.

- Add—Adds an H.323 class map.
- Edit—Edits an H.323 class map.
- Delete—Deletes an H.323 class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit H.323 Match Criterion

The Add/Edit H.323 Match Criterion dialog box lets you define the match criterion and value for the H.323 class map.

### Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of H.323 traffic to match.
  - Called Party—Match the called party.
  - Calling Party—Match the calling party.
  - Media Type—Match the media type.
- Called Party Criterion Values—Specifies to match on the H.323 called party.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match on the H.323 calling party.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Media Type Criterion Values—Specifies which media type to match.

- Audio—Match audio type.
- Video—Match video type.
- Data—Match data type.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## HTTP Class Map

The HTTP Class Map panel lets you configure HTTP class maps for HTTP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- Name—Shows the HTTP class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the HTTP class map.
  - Value—Shows the value to match in the HTTP class map.
- Description—Shows the description of the class map.
- Add—Adds an HTTP class map.
- Edit—Edits an HTTP class map.
- Delete—Deletes an HTTP class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HTTP Traffic Class Map

The Add/Edit HTTP Traffic Class Map dialog box lets you define a HTTP class map.

### Fields

- Name—Enter the name of the HTTP class map, up to 40 characters in length.
- Description—Enter the description of the HTTP class map.
- Add—Adds an HTTP class map.
- Edit—Edits an HTTP class map.
- Delete—Deletes an HTTP class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HTTP Match Criterion

The Add/Edit HTTP Match Criterion dialog box lets you define the match criterion and value for the HTTP class map.

### Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of HTTP traffic to match.
  - Request/Response Content Type Mismatch—Specifies that the content type in the response must match one of the MIME types in the accept field of the request.
  - Request Arguments—Applies the regular expression match to the arguments of the request.  
 Regular Expression—Lists the defined regular expressions to match.  
 Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
 Regular Expression Class—Lists the defined regular expression classes to match.  
 Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - Request Body Length—Applies the regular expression match to the body of the request with field length greater than the bytes specified.  
 Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.

- Request Body—Applies the regular expression match to the body of the request.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request Header Field Count—Applies the regular expression match to the header of the request with a maximum number of header fields.
  - Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Greater Than Count—Enter the maximum number of header fields.
- Request Header Field Length—Applies the regular expression match to the header of the request with field length greater than the bytes specified.
  - Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.
- Request Header Field—Applies the regular expression match to the header of the request.
  - Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.



- Request Header Count—Applies the regular expression match to the header of the request with a maximum number of headers.  
Greater Than Count—Enter the maximum number of headers.
- Request Header Length—Applies the regular expression match to the header of the request with length greater than the bytes specified.  
Greater Than Length—Enter a header length value in bytes.
- Request Header non-ASCII—Matches non-ASCII characters in the header of the request.
- Request Method—Applies the regular expression match to the method of the request.  
Method—Specifies to match on a request method: bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.  
Regular Expression—Specifies to match on a regular expression.  
Regular Expression—Lists the defined regular expressions to match.  
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
Regular Expression Class—Lists the defined regular expression classes to match.  
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request URI Length—Applies the regular expression match to the URI of the request with length greater than the bytes specified.  
Greater Than Length—Enter a URI length value in bytes.
- Request URI—Applies the regular expression match to the URI of the request.  
Regular Expression—Lists the defined regular expressions to match.  
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
Regular Expression Class—Lists the defined regular expression classes to match.  
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Response Body—Applies the regex match to the body of the response.  
ActiveX—Specifies to match on ActiveX.  
Java Applet—Specifies to match on a Java Applet.  
Regular Expression—Specifies to match on a regular expression.  
Regular Expression—Lists the defined regular expressions to match.  
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
Regular Expression Class—Lists the defined regular expression classes to match.  
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Response Body Length—Applies the regular expression match to the body of the response with field length greater than the bytes specified.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field Count—Applies the regular expression match to the header of the response with a maximum number of header fields.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Response Header Field Length—Applies the regular expression match to the header of the response with field length greater than the bytes specified.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field—Applies the regular expression match to the header of the response.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Header Count—Applies the regular expression match to the header of the response with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Response Header Length—Applies the regular expression match to the header of the response with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Response Header non-ASCII—Matches non-ASCII characters in the header of the response.

- Response Status Line—Applies the regular expression match to the status line.
- Regular Expression—Lists the defined regular expressions to match.
- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## IM Class Map

The IM Class Map panel lets you configure IM class maps for IM inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- Name—Shows the IM class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the IM class map.
  - Value—Shows the value to match in the IM class map.
- Description—Shows the description of the class map.
- Add—Adds an IM class map.
- Edit—Edits an IM class map.
- Delete—Deletes an IM class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IM Traffic Class Map

The Add/Edit IM Traffic Class Map dialog box lets you define a IM class map.

### Fields

- Name—Enter the name of the IM class map, up to 40 characters in length.
- Description—Enter the description of the IM class map.
- Add—Adds an IM class map.
- Edit—Edits an IM class map.
- Delete—Deletes an IM class map.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IM Match Criterion

The Add/Edit IM Match Criterion dialog box lets you define the match criterion and value for the IM class map.

### Fields

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of IM traffic to match.
  - Protocol—Match IM protocols.
  - Service—Match IM services.
  - Version—Match IM file transfer service version.
  - Client Login Name—Match client login name from IM service.
  - Client Peer Login Name—Match client peer login name from IM service.

- Source IP Address—Match source IP address.
  - Destination IP Address—Match destination IP address.
  - Filename—Match filename form IM file transfer service.
- Protocol Criterion Values—Specifies which IM protocols to match.
  - Yahoo! Messenger—Specifies to match Yahoo! Messenger instant messages.
  - MSN Messenger—Specifies to match MSN Messenger instant messages.
- Service Criterion Values—Specifies which IM services to match.
  - Chat—Specifies to match IM message chat service.
  - Conference—Specifies to match IM conference service.
  - File Transfer—Specifies to match IM file transfer service.
  - Games—Specifies to match IM gaming service.
  - Voice Chat—Specifies to match IM voice chat service (not available for Yahoo IM)
  - Web Cam—Specifies to match IM webcam service.
- Version Criterion Values—Specifies to match the version from the IM file transfer service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Login Name Criterion Values—Specifies to match the client login name from the IM service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Peer Login Name Criterion Values—Specifies to match the client peer login name from the IM service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Source IP Address Criterion Values—Specifies to match the source IP address of the IM service.
  - IP Address—Enter the source IP address of the IM service.
  - IP Mask—Mask of the source IP address.

- **Destination IP Address Criterion Values**—Specifies to match the destination IP address of the IM service.
  - **IP Address**—Enter the destination IP address of the IM service.
  - **IP Mask**—Mask of the destination IP address.
- **Filename Criterion Values**—Specifies to match the filename from the IM file transfer service. Applies the regular expression match.
  - **Regular Expression**—Lists the defined regular expressions to match.
  - **Manage**—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - **Regular Expression Class**—Lists the defined regular expression classes to match.
  - **Manage**—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SIP Class Map

The SIP Class Map panel lets you configure SIP class maps for SIP inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, IM, and SIP.

### Fields

- **Name**—Shows the SIP class map name.
- **Match Conditions**—Shows the type, match criterion, and value in the class map.
  - **Match Type**—Shows the match type, which can be a positive or negative match.
  - **Criterion**—Shows the criterion of the SIP class map.
  - **Value**—Shows the value to match in the SIP class map.
- **Description**—Shows the description of the class map.
- **Add**—Adds a SIP class map.
- **Edit**—Edits a SIP class map.
- **Delete**—Deletes a SIP class map.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SIP Traffic Class Map

The Add/Edit SIP Traffic Class Map dialog box lets you define a SIP class map.

**Fields**

- Name—Enter the name of the SIP class map, up to 40 characters in length.
- Description—Enter the description of the SIP class map.
- Add—Adds a SIP class map.
- Edit—Edits a SIP class map.
- Delete—Deletes a SIP class map.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SIP Match Criterion

The Add/Edit SIP Match Criterion dialog box lets you define the match criterion and value for the SIP class map.

**Fields**

- Match Type—Specifies whether the class map includes traffic that matches the criterion, or traffic that does not match the criterion.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- Criterion—Specifies which criterion of SIP traffic to match.
  - Called Party—Match the called party as specified in the To header.
  - Calling Party—Match the calling party as specified in the From header.
  - Content Length—Match the Content Length header, between 0 and 65536.

- Content Type—Match the Content Type header.
- IM Subscriber—Match the SIP IM subscriber.
- Message Path—Match the SIP Via header.
- Request Method—Match the SIP request method.
- Third-Party Registration—Match the requester of a third-party registration.
- URI Length—Match a URI in the SIP headers, between 0 and 65536.
- Called Party Criterion Values—Specifies to match the called party. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match the calling party. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Content Length Criterion Values—Specifies to match a SIP content header of a length greater than specified.
  - Greater Than Length—Enter a header length value in bytes.
- Content Type Criterion Values—Specifies to match a SIP content header type.
  - SDP—Match an SDP SIP content header type.
  - Regular Expression—Match a regular expression.
    - Regular Expression—Lists the defined regular expressions to match.
    - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
    - Regular Expression Class—Lists the defined regular expression classes to match.
    - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- IM Subscriber Criterion Values—Specifies to match the IM subscriber. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.



- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Message Path Criterion Values—Specifies to match a SIP Via header. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request Method Criterion Values—Specifies to match a SIP request method.
  - Request Method—Specifies a request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- Third-Party Registration Criterion Values—Specifies to match the requester of a third-party registration. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URI Length Criterion Values—Specifies to match a URI of a selected type and greater than the specified length in the SIP headers.
  - URI type—Specifies to match either SIP URI or TEL URI.
  - Greater Than Length—Length in bytes.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Inspect Map Field Descriptions

This section describes how to configure inspect maps, and includes the following topics.



### Note

For information about RADIUS inspect maps, see the [“Adding a Service Policy Rule for Management Traffic” section on page 22-10](#).

- [DCERPC Inspect Map, page 24-62](#)

- [DNS Inspect Map, page 24-64](#)
- [ESMTP Inspect Map, page 24-71](#)
- [FTP Inspect Map, page 24-79](#)
- [GTP Inspect Map, page 24-84](#)
- [H.323 Inspect Map, page 24-89](#)
- [HTTP Inspect Map, page 24-95](#)
- [Instant Messaging \(IM\) Inspect Map, page 24-103](#)
- [IPSec Pass Through Inspect Map, page 24-106](#)
- [MGCP Inspect Map, page 24-109](#)
- [NetBIOS Inspect Map, page 24-112](#)
- [RTSP Inspect Map, page 24-113](#)
- [SCCP \(Skinny\) Inspect Map, page 24-115](#)
- [SIP Inspect Map, page 24-120](#)
- [SNMP Inspect Map, page 24-126](#)

The algorithm the security appliance uses for stateful application inspection ensures the security of applications and services. Some applications require special handling, and specific application inspection engines are provided for this purpose. Applications that require special application inspection engines are those that embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports.

Application inspection engines work with NAT to help identify the location of embedded addressing information. This allows NAT to translate these embedded addresses and to update any checksum or other fields that are affected by the translation.

Each application inspection engine also monitors sessions to determine the port numbers for secondary channels. Many protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection engine monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

In addition, stateful application inspection audits the validity of the commands and responses within the protocol being inspected. The security appliance helps to prevent attacks by verifying that traffic conforms to the RFC specifications for each protocol that is inspected.

The Inspect Maps feature lets you create inspect maps for specific protocol inspection engines. You use an inspect map to store the configuration for a protocol inspection engine. You then enable the configuration settings in the inspect map by associating the map with a specific type of traffic using a global security policy or a security policy for a specific interface.

Use the Service Policy Rules tab on the Security Policy pane to apply the inspect map to traffic matching the criteria specified in the service policy. A service policy can apply to a specific interface or to all the interfaces on the security appliance.

|                    |                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCERPC             | The DCERPC inspection lets you create, view, and manage DCERPC inspect maps. You can use a DCERPC map to inspect DCERPC messages between a client and endpoint mapper, and to apply NAT for the secondary connection, if needed. DCERPC is a specification for a remote procedure call mechanism.                                                                              |
| DNS                | The DNS inspection lets you create, view, and manage DNS inspect maps. You can use a DNS map to have more control over DNS messages and to protect against DNS spoofing and cache poisoning. DNS is used to resolve information about domain names, including IP addresses and mail servers.                                                                                   |
| ESMTP              | The ESMTP inspection lets you create, view, and manage ESMTP inspect maps. You can use an ESMTP map for application security and protocol conformance to protect against attacks, to block senders and receivers, and to block mail relay. Extended SMTP defines protocol extensions to the SMTP standard.                                                                     |
| FTP                | The FTP inspection lets you create, view, and manage FTP inspect maps. FTP is a common protocol used for transferring files over a TCP/IP network, such as the Internet. You can use an FTP map to block specific FTP protocol methods, such as an FTP PUT, from passing through the security appliance and reaching your FTP server.                                          |
| GTP                | The GTP inspection lets you create, view, and manage GTP inspect maps. GTP is a relatively new protocol designed to provide security for wireless connections to TCP/IP networks, such as the Internet. You can use a GTP map to control timeout values, message sizes, tunnel counts, and GTP versions traversing the security appliance.                                     |
| H.323              | The H.323 inspection lets you create, view, and manage H.323 inspect maps. You can use an H.323 map to inspect RAS, H.225, and H.245 VoIP protocols, and for state tracking and filtering.                                                                                                                                                                                     |
| HTTP               | The HTTP inspection lets you create, view, and manage HTTP inspect maps. HTTP is the protocol used for communication between Worldwide Web clients and servers. You can use an HTTP map to enforce RFC compliance and HTTP payload content type. You can also block specific HTTP methods and prevent the use of certain tunneled applications that use HTTP as the transport. |
| IM                 | The IM inspection lets you create, view, and manage IM inspect maps. You can use an IM map to control the network usage and stop leakage of confidential data and other network threats from IM applications.                                                                                                                                                                  |
| IPSec Pass Through | The IPSec Pass Through inspection lets you create, view, and manage IPSec Pass Through inspect maps. You can use an IPSec Pass Through map to permit certain flows without using an access list.                                                                                                                                                                               |
| MGCP               | The MGCP inspection lets you create, view, and manage MGCP inspect maps. You can use an MGCP map to manage connections between VoIP devices and MGCP call agents.                                                                                                                                                                                                              |
| NetBIOS            | The NetBIOS inspection lets you create, view, and manage NetBIOS inspect maps. You can use a NetBIOS map to enforce NetBIOS protocol conformance including field count and length consistency, and message checks.                                                                                                                                                             |

|                   |                                                                                                                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS Accounting | The RADIUS Accounting inspection lets you create, view, and manage RADIUS Accounting inspect maps. You can use a RADIUS map to protect against an overbilling attack.                                                                                                                                          |
| RTSP              | The RTSP inspection lets you create, view, and manage RTSP inspect maps. You can use an RTSP map to protect RTSP traffic, including RTSP PAT.                                                                                                                                                                  |
| SCCP (Skinny)     | The SCCP (Skinny) inspection lets you create, view, and manage SCCP (Skinny) inspect maps. You can use an SCCP map to perform protocol conformance checks and basic state tracking.                                                                                                                            |
| SIP               | The SIP inspection lets you create, view, and manage SIP inspect maps. You can use a SIP map for application security and protocol conformance to protect against SIP-based attacks. SIP is a protocol widely used for internet conferencing, telephony, presence, events notification, and instant messaging. |
| SNMP              | The SNMP inspection lets you create, view, and manage SNMP inspect maps. SNMP is a protocol used for communication between network management devices and network management stations. You can use an SNMP map to block a specific SNMP version, including SNMP v1, 2, 2c and 3.                               |

## DCERPC Inspect Map

The DCERPC pane lets you view previously configured DCERPC application inspection maps. A DCERPC map lets you change the default configuration values used for DCERPC application inspection.

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper (EPM) listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The security appliance allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.

DCERPC inspect maps inspect for native TCP communication between the EPM and client on well known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have user configurable timeouts.

### Fields

- DCERPC Inspect Maps—Table that lists the defined DCERPC inspect maps.
- Add—Configures a new DCERPC inspect map. To edit a DCERPC inspect map, select the DCERPC entry in the DCERPC Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the DCERPC Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
  - Low
    - Pinhole timeout: 00:02:00
    - Endpoint mapper service: not enforced

- Endpoint mapper service lookup: enabled
- Endpoint mapper service lookup timeout: 00:05:00
- Medium—Default.
  - Pinhole timeout: 00:01:00
  - Endpoint mapper service: not enforced
  - Endpoint mapper service lookup: disabled.
- High
  - Pinhole timeout: 00:01:00
  - Endpoint mapper service: enforced
  - Endpoint mapper service lookup: disabled
- Customize—Opens the Add/Edit DCERPC Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Medium.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit DCERPC Policy Map

The Add/Edit DCERPC Policy Map pane lets you configure the security level and parameters for DCERPC application inspection maps.

### Fields

- Name—When adding a DCERPC map, enter the name of the DCERPC map. When editing a DCERPC map, the name of the previously configured DCERPC map is shown.
- Description—Enter the description of the DCERPC map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
  - Low
    - Pinhole timeout: 00:02:00
    - Endpoint mapper service: not enforced
    - Endpoint mapper service lookup: enabled
    - Endpoint mapper service lookup timeout: 00:05:00
  - Medium—Default.
    - Pinhole timeout: 00:01:00
    - Endpoint mapper service: not enforced
    - Endpoint mapper service lookup: disabled.

- High
  - Pinhole timeout: 00:01:00
  - Endpoint mapper service: enforced
  - Endpoint mapper service lookup: disabled
- Default Level—Sets the security level back to the default level of Medium.
- Details—Shows the Parameters to configure additional settings.
  - Pinhole Timeout—Sets the pinhole timeout. Since a client may use the server information returned by the endpoint mapper for multiple connections, the timeout value is configurable based on the client application environment. Range is from 0:0:1 to 1193:0:0. Default is 2 minutes.
  - Enforce endpoint-mapper service—Enforces endpoint mapper service during binding.
  - Enable endpoint-mapper service lookup—Enables the lookup operation of the endpoint mapper service. If disabled, the pinhole timeout is used.
  - Enforce Service Lookup Timeout—Enforces the service lookup timeout specified.
  - Service Lookup Timeout—Sets the timeout for pinholes from lookup operation.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## DNS Inspect Map

The DNS pane lets you view previously configured DNS application inspection maps. A DNS map lets you change the default configuration values used for DNS application inspection.

DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow certain DNS types to be allowed, dropped, and/or logged, while others are blocked. Zone transfer can be restricted between servers with this function, for example.

The Recursion Desired and Recursion Available flags in the DNS header can be masked to protect a public server from attack if that server only supports a particular internal zone. In addition, DNS randomization can be enabled to avoid spoofing and cache poisoning of servers that either do not support randomization, or utilize a weak pseudo random number generator. Limiting the domain names that can be queried also restricts the domain names which can be queried, which protects the public server further.

A configurable DNS mismatch alert can be used as notification if an excessive number of mismatching DNS responses are received, which could indicate a cache poisoning attack. In addition, a configurable check to enforce a Transaction Signature be attached to all DNS messages is also supported.

### Fields

- DNS Inspect Maps—Table that lists the defined DNS inspect maps.

- Add—Configures a new DNS inspect map. To edit a DNS inspect map, select the DNS entry in the DNS Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the DNS Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
  - Low—Default.
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: disabled
    - Message length check: enabled
    - Message length maximum: 512
    - Mismatch rate logging: disabled
    - TSIG resource record: not enforced
  - Medium
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: enabled
    - Message length check: enabled
    - Message length maximum: 512
    - Mismatch rate logging: enabled
    - TSIG resource record: not enforced
  - High
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: enabled
    - Message length check: enabled
    - Message length maximum: 512
    - Mismatch rate logging: enabled
    - TSIG resource record: enforced
- Customize—Opens the Add/Edit DNS Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit DNS Policy Map (Security Level)

The Add/Edit DNS Policy Map pane lets you configure the security level and additional settings for DNS application inspection maps.

### Fields

- Name—When adding a DNS map, enter the name of the DNS map. When editing a DNS map, the name of the previously configured DNS map is shown.
- Description—Enter the description of the DNS map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
  - Low—Default.
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: disabled
    - Message length check: enabled
    - Message length maximum: 512
    - Mismatch rate logging: disabled
    - TSIG resource record: not enforced
  - Medium
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: enabled
    - Message length check: enabled
    - Message length maximum: 512
    - Mismatch rate logging: enabled
    - TSIG resource record: not enforced
  - High
    - DNS Guard: enabled
    - NAT rewrite: enabled
    - Protocol enforcement: enabled
    - ID randomization: enabled



Message length check: enabled

Message length maximum: 512

Mismatch rate logging: enabled

TSIG resource record: enforced

- Default Level—Sets the security level back to the default level of Low.

- Details—Shows the Protocol Conformance, Filtering, Mismatch Rate, and Inspection tabs to configure additional settings.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit DNS Policy Map (Details)

The Add/Edit DNS Policy Map pane lets you configure the security level and additional settings for DNS application inspection maps.

### Fields

- Name—When adding a DNS map, enter the name of the DNS map. When editing a DNS map, the name of the previously configured DNS map is shown.
- Description—Enter the description of the DNS map, up to 200 characters in length.
- Security Level—Shows the security level to configure.
- Protocol Conformance—Tab that lets you configure the protocol conformance settings for DNS.
  - Enable DNS guard function—Performs a DNS query and response mismatch check using the identification field in the DNS header. One response per query is allowed to go through the security appliance.
  - Enable NAT re-write function—Enables IP address translation in the A record of the DNS response.
  - Enable protocol enforcement—Enables DNS message format check, including domain name, label length, compression, and looped pointer check.
  - Randomize the DNS identifier for DNS query—Randomizes the DNS identifier in the DNS query message.
  - Enforce TSIG resource record to be present in DNS message—Requires that a TSIG resource record be present in DNS transactions. Actions taken when TSIG is enforced:
    - Drop packet—Drops the packet (logging can be either enabled or disabled).
    - Log—Enables logging.
- Filtering—Tab that lets you configure the filtering settings for DNS.
  - Global Settings—Applies settings globally.

Drop packets that exceed specified maximum length (global)—Drops packets that exceed maximum length in bytes.

Maximum Packet Length—Enter maximum packet length in bytes.

- Server Settings—Applies settings on the server only.

Drop packets that exceed specified maximum length—Drops packets that exceed maximum length in bytes.

Maximum Packet Length—Enter maximum packet length in bytes.

Drop packets sent to server that exceed length indicated by the RR—Drops packets sent to the server that exceed the length indicated by the Resource Record.

- Client Settings—Applies settings on the client only.

Drop packets that exceed specified maximum length—Drops packets that exceed maximum length in bytes.

Maximum Packet Length—Enter maximum packet length in bytes.

Drop packets sent to client that exceed length indicated by the RR—Drops packets sent to the client that exceed the length indicated by the Resource Record.

- Mismatch Rate—Tab that lets you configure the ID mismatch rate for DNS.
  - Enable Logging when DNS ID mismatch rate exceeds specified rate—Reports excessive instances of DNS identifier mismatches.

Mismatch Instance Threshold—Enter the maximum number of mismatch instances before a system message log is sent.

Time Interval—Enter the time period to monitor (in seconds).
- Inspections—Tab that shows you the DNS inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the DNS inspection.
  - Value—Shows the value to match in the DNS inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add DNS Inspect dialog box to add a DNS inspection.
  - Edit—Opens the Edit DNS Inspect dialog box to edit a DNS inspection.
  - Delete—Deletes a DNS inspection.
  - Move Up—Moves an inspection up in the list.
  - Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit DNS Inspect

The Add/Edit DNS Inspect dialog box lets you define the match criterion and value for the DNS inspect map.

### Fields

- **Single Match**—Specifies that the DNS inspect has only one match statement.
- **Match Type**—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- **Criterion**—Specifies which criterion of DNS traffic to match.
  - **Header Flag**—Match a DNS flag in the header.
  - **Type**—Match a DNS query or resource record type.
  - **Class**—Match a DNS query or resource record class.
  - **Question**—Match a DNS question.
  - **Resource Record**—Match a DNS resource record.
  - **Domain Name**—Match a domain name from a DNS query or resource record.
- **Header Flag Criterion Values**—Specifies the value details for DNS header flag match.
  - **Match Option**—Specifies either an exact match or match all bits (bit mask match).
  - **Match Value**—Specifies to match either the header flag name or the header flag value.  
**Header Flag Name**—Lets you select one or more header flag names to match, including AA (authoritative answer), QR (query), RA (recursion available), RD (recursion denied), TC (truncation) flag bits.  
**Header Flag Value**—Lets you enter an arbitrary 16-bit value in hex to match.
- **Type Criterion Values**—Specifies the value details for DNS type match.
  - **DNS Type Field Name**—Lists the DNS types to select.  
 A—IPv4 address  
 NS—Authoritative name server  
 CNAME—Canonical name  
 SOA—Start of a zone of authority  
 TSIG—Transaction signature  
 IXFR—Incremental (zone) transfer  
 AXFR—Full (zone) transfer
  - **DNS Type Field Value**—Specifies to match either a DNS type field value or a DNS type field range.  
**Value**—Lets you enter an arbitrary value between 0 and 65535 to match.  
**Range**—Lets you enter a range match. Both values between 0 and 65535.
- **Class Criterion Values**—Specifies the value details for DNS class match.
  - **DNS Class Field Name**—Specifies to match on internet, the DNS class field name.

- DNS Class Field Value—Specifies to match either a DNS class field value or a DNS class field range.
  - Value—Lets you enter an arbitrary value between 0 and 65535 to match.
  - Range—Lets you enter a range match. Both values between 0 and 65535.
- Question Criterion Values—Specifies to match on the DNS question section.
- Resource Record Criterion Values—Specifies to match on the DNS resource record section.
  - Resource Record—Lists the sections to match.
    - Additional—DNS additional resource record
    - Answer—DNS answer resource record
    - Authority—DNS authority resource record
- Domain Name Criterion Values—Specifies to match on DNS domain name.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Multiple Matches—Specifies multiple matches for the DNS inspection.
  - DNS Traffic Class—Specifies the DNS traffic class match.
  - Manage—Opens the Manage DNS Class Maps dialog box to add, edit, or delete DNS Class Maps.
- Actions—Primary action and log settings.
  - Primary Action—Mask, drop packet, drop connection, none.
  - Log—Enable or disable.
  - Enforce TSIG—Do not enforce, drop packet, log, drop packet and log.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Manage Class Maps

The Manage Class Map dialog box lets you configure class maps for inspection.

An inspection class map matches application traffic with criteria specific to the application. You then identify the class map in the inspect map and enable actions. The difference between creating a class map and defining the traffic match directly in the inspect map is that you can create more complex match criteria and you can reuse class maps. The applications that support inspection class maps are DNS, FTP, H.323, HTTP, Instant Messaging (IM), and SIP.

#### Fields

- Name—Shows the class map name.
- Match Conditions—Shows the type, match criterion, and value in the class map.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the class map.
  - Value—Shows the value to match in the class map.
- Description—Shows the description of the class map.
- Add—Adds match conditions for the class map.
- Edit—Edits match conditions for the class map.
- Delete—Deletes match conditions for the class map.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## ESMTP Inspect Map

The ESMTP pane lets you view previously configured ESMTP application inspection maps. An ESMTP map lets you change the default configuration values used for ESMTP application inspection.

Since ESMTP traffic can be a main source of attack from spam, phishing, malformed messages, buffer overflows, and buffer underflows, detailed packet inspection and control of ESMTP traffic are supported. Application security and protocol conformance enforce the sanity of the ESMTP message as well as detect several attacks, block senders and receivers, and block mail relay.

#### Fields

- ESMTP Inspect Maps—Table that lists the defined ESMTP inspect maps.
- Add—Configures a new ESMTP inspect map. To edit an ESMTP inspect map, select the ESMTP entry in the ESMTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the ESMTP Inspect Maps table.
- Security Level—Select the security level (high, medium, or low).
  - Low—Default.
    - Log if command line length is greater than 512
    - Log if command recipient count is greater than 100

- Log if body line length is greater than 1000
- Log if sender address length is greater than 320
- Log if MIME file name length is greater than 255
- Medium
  - Obfuscate Server Banner
  - Drop Connections if command line length is greater than 512
  - Drop Connections if command recipient count is greater than 100
  - Drop Connections if body line length is greater than 1000
  - Drop Connections if sender address length is greater than 320
  - Drop Connections if MIME file name length is greater than 255
- High
  - Obfuscate Server Banner
  - Drop Connections if command line length is greater than 512
  - Drop Connections if command recipient count is greater than 100
  - Drop Connections if body line length is greater than 1000
  - Drop Connections and log if sender address length is greater than 320
  - Drop Connections and log if MIME file name length is greater than 255
- MIME File Type Filtering—Opens the MIME Type Filtering dialog box to configure MIME file type filters.
- Customize—Opens the Add/Edit ESMTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## MIME File Type Filtering

The MIME File Type Filtering dialog box lets you configure the settings for a MIME file type filter.

### Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.

- Add—Opens the Add MIME File Type Filter dialog box to add a MIME file type filter.
- Edit—Opens the Edit MIME File Type Filter dialog box to edit a MIME file type filter.
- Delete—Deletes a MIME file type filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit ESMTP Policy Map (Security Level)

The Add/Edit ESMTP Policy Map pane lets you configure the security level and additional settings for ESMTP application inspection maps.

### Fields

- Name—When adding an ESMTP map, enter the name of the ESMTP map. When editing an ESMTP map, the name of the previously configured ESMTPS map is shown.
- Description—Enter the description of the ESMTP map, up to 200 characters in length.
- Security Level—Select the security level (high, medium, or low).
  - Low—Default.
    - Log if command line length is greater than 512
    - Log if command recipient count is greater than 100
    - Log if body line length is greater than 1000
    - Log if sender address length is greater than 320
    - Log if MIME file name length is greater than 255
  - Medium
    - Obfuscate Server Banner
    - Drop Connections if command line length is greater than 512
    - Drop Connections if command recipient count is greater than 100
    - Drop Connections if body line length is greater than 1000
    - Drop Connections if sender address length is greater than 320
    - Drop Connections if MIME file name length is greater than 255
  - High
    - Obfuscate Server Banner
    - Drop Connections if command line length is greater than 512

- Drop Connections if command recipient count is greater than 100
- Drop Connections if body line length is greater than 1000
- Drop Connections and log if sender address length is greater than 320
- Drop Connections and log if MIME file name length is greater than 255
- MIME File Type Filtering—Opens the MIME Type Filtering dialog box to configure MIME file type filters.
- Default Level—Sets the security level back to the default level of Low.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit ESMTP Policy Map (Details)

The Add/Edit ESMTP Policy Map pane lets you configure the security level and additional settings for ESMTP application inspection maps.

### Fields

- Name—When adding an ESMTP map, enter the name of the ESMTP map. When editing an ESMTP map, the name of the previously configured ESMTP map is shown.
- Description—Enter the description of the ESMTP map, up to 200 characters in length.
- Security Level—Shows the security level and mime file type filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the ESMTP inspect map.
  - Mask server banner—Enforces banner obfuscation.
  - Configure Mail Relay—Enables ESMTP mail relay.
  - Domain Name—Specifies a local domain.
  - Action—Drop connection or log.
  - Log—Enable or disable.
- Inspections—Tab that shows you the ESMTP inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the ESMTP inspection.
  - Value—Shows the value to match in the ESMTP inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add ESMTP Inspect dialog box to add an ESMTP inspection.



- Edit—Opens the Edit ESMTP Inspect dialog box to edit an ESMTP inspection.
- Delete—Deletes an ESMTP inspection.
- Move Up—Moves an inspection up in the list.
- Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit ESMTP Inspect

The Add/Edit ESMTP Inspect dialog box lets you define the match criterion and value for the ESMTP inspect map.

### Fields

- Match Type—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of ESMTP traffic to match.
  - Body Length—Match body length at specified length in bytes.
  - Body Line Length—Match body line length matching at specified length in bytes.
  - Commands—Match commands exchanged in the ESMTP protocol.
  - Command Recipient Count—Match command recipient count greater than number specified.
  - Command Line Length—Match command line length greater than length specified in bytes.
  - EHLO Reply Parameters—Match an ESMTP ehlo reply parameter.
  - Header Length—Match header length at length specified in bytes.
  - Header To Fields Count—Match header To fields count greater than number specified.
  - Invalid Recipients Count—Match invalid recipients count greater than number specified.
  - MIME File Type—Match MIME file type.
  - MIME Filename Length—Match MIME filename.
  - MIME Encoding—Match MIME encoding.
  - Sender Address—Match sender email address.
  - Sender Address Length—Match sender email address length.
- Body Length Criterion Values—Specifies the value details for body length match.
  - Greater Than Length—Body length in bytes.
  - Action—Reset, drop connection, log.

- Log—Enable or disable.
- Body Line Length Criterion Values—Specifies the value details for body line length match.
  - Greater Than Length—Body line length in bytes.
  - Action—Reset, drop connection, log.
  - Log—Enable or disable.
- Commands Criterion Values—Specifies the value details for command match.
  - Available Commands Table:
    - AUTH
    - DATA
    - EHLO
    - ETRN
    - HELO
    - HELP
    - MAIL
    - NOOP
    - QUIT
    - RCPT
    - RSET
    - SAML
    - SOML
    - VRFY
  - Add—Adds the selected command from the Available Commands table to the Selected Commands table.
  - Remove—Removes the selected command from the Selected Commands table.
  - Primary Action—Mask, Reset, Drop Connection, None, Limit Rate (pps).
  - Log—Enable or disable.
  - Rate Limit—Do not limit rate, Limit Rate (pps).
- Command Recipient Count Criterion Values—Specifies the value details for command recipient count match.
  - Greater Than Count—Specify command recipient count.
  - Action—Reset, drop connection, log.
  - Log—Enable or disable.
- Command Line Length Criterion Values—Specifies the value details for command line length.
  - Greater Than Length—Command line length in bytes.
  - Action—Reset, drop connection, log.
  - Log—Enable or disable.
- EHLO Reply Parameters Criterion Values—Specifies the value details for EHLO reply parameters match.

- Available Parameters Table:
  - 8bitmime
  - auth
  - binarymime
  - checkpoint
  - dsn
  - ecode
  - etrn
  - others
  - pipelining
  - size
  - vrfy
- Add—Adds the selected parameter from the Available Parameters table to the Selected Parameters table.
- Remove—Removes the selected command from the Selected Commands table.
- Action—Reset, Drop Connection, Mask, Log.
- Log—Enable or disable.
- Header Length Criterion Values—Specifies the value details for header length match.
  - Greater Than Length—Header length in bytes.
  - Action—Reset, Drop Connection, Mask, Log.
  - Log—Enable or disable.
- Header To Fields Count Criterion Values—Specifies the value details for header To fields count match.
  - Greater Than Count—Specify command recipient count.
  - Action—Reset, drop connection, log.
  - Log—Enable or disable.
- Invalid Recipients Count Criterion Values—Specifies the value details for invalid recipients count match.
  - Greater Than Count—Specify command recipient count.
  - Action—Reset, drop connection, log.
  - Log—Enable or disable.
- MIME File Type Criterion Values—Specifies the value details for MIME file type match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - Action—Reset, drop connection, log.

- Log—Enable or disable.
- MIME Filename Length Criterion Values—Specifies the value details for MIME filename length match.
  - Greater Than Length—MIME filename length in bytes.
  - Action—Reset, Drop Connection, Log.
  - Log—Enable or disable.
- MIME Encoding Criterion Values—Specifies the value details for MIME encoding match.
  - Available Encodings table
    - 7bit
    - 8bit
    - base64
    - binary
    - others
    - quoted-printable
  - Add—Adds the selected parameter from the Available Encodings table to the Selected Encodings table.
  - Remove—Removes the selected command from the Selected Commands table.
  - Action—Reset, Drop Connection, Log.
  - Log—Enable or disable.
- Sender Address Criterion Values—Specifies the value details for sender address match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - Action—Reset, Drop Connection, Log.
  - Log—Enable or disable.
- Sender Address Length Criterion Values—Specifies the value details for sender address length match.
  - Greater Than Length—Sender address length in bytes.
  - Action—Reset, Drop Connection, Log.
  - Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## FTP Inspect Map

The FTP pane lets you view previously configured FTP application inspection maps. An FTP map lets you change the default configuration values used for FTP application inspection.

FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation.

Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download, but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.

### Fields

- FTP Inspect Maps—Table that lists the defined FTP inspect maps.
- Add—Configures a new FTP inspect map. To edit an FTP inspect map, select the FTP entry in the FTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the FTP Inspect Maps table.
- Security Level—Select the security level (medium or low).
  - Low
    - Mask Banner Disabled
    - Mask Reply Disabled
  - Medium—Default.
    - Mask Banner Enabled
    - Mask Reply Enabled
  - File Type Filtering—Opens the Type Filtering dialog box to configure file type filters.
  - Customize—Opens the Add/Edit FTP Policy Map dialog box for additional settings.
  - Default Level—Sets the security level back to the default level of Medium.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## File Type Filtering

The File Type Filtering dialog box lets you configure the settings for a file type filter.

### Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add File Type Filter dialog box to add a file type filter.
- Edit—Opens the Edit File Type Filter dialog box to edit a file type filter.
- Delete—Deletes a file type filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit FTP Policy Map (Security Level)

The Add/Edit FTP Policy Map pane lets you configure the security level and additional settings for FTP application inspection maps.

### Fields

- Name—When adding an FTP map, enter the name of the FTP map. When editing an FTP map, the name of the previously configured FTP map is shown.
- Description—Enter the description of the FTP map, up to 200 characters in length.
- Security Level—Select the security level (medium or low).
  - Low
    - Mask Banner Disabled
    - Mask Reply Disabled
  - Medium—Default.
    - Mask Banner Enabled
    - Mask Reply Enabled
  - File Type Filtering—Opens the Type Filtering dialog box to configure file type filters.

- Default Level—Sets the security level back to the default level of Medium.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit FTP Policy Map (Details)

The Add/Edit FTP Policy Map pane lets you configure the security level and additional settings for FTP application inspection maps.

### Fields

- Name—When adding an FTP map, enter the name of the FTP map. When editing an FTP map, the name of the previously configured FTP map is shown.
- Description—Enter the description of the FTP map, up to 200 characters in length.
- Security Level—Shows the security level and file type filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the FTP inspect map.
  - Mask greeting banner from the server—Masks the greeting banner from the FTP server to prevent the client from discovering server information.
  - Mask reply to SYST command—Masks the reply to the syst command to prevent the client from discovering server information.
- Inspections—Tab that shows you the FTP inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the FTP inspection.
  - Value—Shows the value to match in the FTP inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add FTP Inspect dialog box to add an FTP inspection.
  - Edit—Opens the Edit FTP Inspect dialog box to edit an FTP inspection.
  - Delete—Deletes an FTP inspection.
  - Move Up—Moves an inspection up in the list.
  - Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit FTP Map

The Add/Edit FTP Inspect dialog box lets you define the match criterion and value for the FTP inspect map.

### Fields

- Single Match—Specifies that the FTP inspect has only one match statement.
- Match Type—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of FTP traffic to match.
  - Request Command—Match an FTP request command.
  - File Name—Match a filename for FTP transfer.
  - File Type—Match a file type for FTP transfer.
  - Server—Match an FTP server.
  - User Name—Match an FTP user.
- Request Command Criterion Values—Specifies the value details for FTP request command match.
  - Request Command:
    - APPE—Command that appends to a file.
    - CDUP—Command that changes to the parent directory of the current working directory.
    - DELE—Command that deletes a file.
    - GET—Command that gets a file.
    - HELP—Command that provides help information.
    - MKD—Command that creates a directory.
    - PUT—Command that sends a file.
    - RMD—Command that deletes a directory.
    - RNFR—Command that specifies rename-from filename.
    - RNTO—Command that specifies rename-to filename.
    - SITE—Commands that are specific to the server system. Usually used for remote administration.
    - STOU—Command that stores a file using a unique filename.
- File Name Criterion Values—Specifies the value details for FTP filename match.
  - Regular Expression—Lists the defined regular expressions to match.



- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- File Type Criterion Values—Specifies the value details for FTP file type match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Server Criterion Values—Specifies the value details for FTP server match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- User Name Criterion Values—Specifies the value details for FTP user name match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Multiple Matches—Specifies multiple matches for the FTP inspection.
  - FTP Traffic Class—Specifies the FTP traffic class match.
  - Manage—Opens the Manage FTP Class Maps dialog box to add, edit, or delete FTP Class Maps.
- Action—Reset.
- Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## GTP Inspect Map

The GTP pane lets you view previously configured GTP application inspection maps. A GTP map lets you change the default configuration values used for GTP application inspection.

GTP is a relatively new protocol designed to provide security for wireless connections to TCP/IP networks, such as the Internet. You can use a GTP map to control timeout values, message sizes, tunnel counts, and GTP versions traversing the security appliance.



**Note** GTP inspection is not available without a special license.

### Fields

- GTP Inspect Maps—Table that lists the defined GTP inspect maps.
- Add—Configures a new GTP inspect map. To edit a GTP inspect map, select the GTP entry in the GTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the GTP Inspect Maps table.
- Security Level—Security level low only.
  - Do not Permit Errors
  - Maximum Number of Tunnels: 500
  - GSN timeout: 00:30:00
  - Pdp-Context timeout: 00:30:00
  - Request timeout: 00:01:00
  - Signaling timeout: 00:30:00.
  - Tunnel timeout: 01:00:00.
  - T3-response timeout: 00:00:20.
  - Drop and log unknown message IDs.
- IMSI Prefix Filtering—Opens the IMSI Prefix Filtering dialog box to configure IMSI prefix filters.
- Customize—Opens the Add/Edit GTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## IMSI Prefix Filtering

The IMSI Prefix tab lets you define the IMSI prefix to allow within GTP requests.

**Fields**

- **Mobile Country Code**—Defines the non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
- **Mobile Network Code**—Defines the two or three-digit value identifying the network code.
- **Add**—Add the specified country code and network code to the IMSI Prefix table.
- **Delete**—Deletes the specified country code and network code from the IMSI Prefix table.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit GTP Policy Map (Security Level)

The Add/Edit GTP Policy Map pane lets you configure the security level and additional settings for GTP application inspection maps.

**Fields**

- **Name**—When adding a GTP map, enter the name of the GTP map. When editing a GTP map, the name of the previously configured GTP map is shown.
- **Description**—Enter the description of the GTP map, up to 200 characters in length.
- **Security Level**—Security level low only.
  - Do not Permit Errors
  - Maximum Number of Tunnels: 500
  - GSN timeout: 00:30:00
  - Pdp-Context timeout: 00:30:00
  - Request timeout: 00:01:00
  - Signaling timeout: 00:30:00.
  - Tunnel timeout: 01:00:00.
  - T3-response timeout: 00:00:20.
  - Drop and log unknown message IDs.
  - **IMSI Prefix Filtering**—Opens the IMSI Prefix Filtering dialog box to configure IMSI prefix filters.
  - **Default Level**—Sets the security level back to the default.
- **Details**—Shows the Parameters, IMSI Prefix Filtering, and Inspections tabs to configure additional settings.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit GTP Policy Map (Details)

The Add/Edit GTP Policy Map pane lets you configure the security level and additional settings for GTP application inspection maps.

### Fields

- **Name**—When adding a GTP map, enter the name of the GTP map. When editing a GTP map, the name of the previously configured GTP map is shown.
- **Description**—Enter the description of the GTP map, up to 200 characters in length.
- **Security Level**—Shows the security level and IMSI prefix filtering settings to configure.
- **Permit Parameters**—Tab that lets you configure the permit parameters for the GTP inspect map.
  - **Object Groups to Add**
    - From object group—Specify an object group or use the browse button to open the Add Network Object Group dialog box.
    - To object group—Specify an object group or use the browse button to open the Add Network Object Group dialog box.
  - **Add**—Add the specified country code and network code to the IMSI Prefix table.
  - **Delete**—Deletes the specified country code and network code from the IMSI Prefix table.
  - **Permit Errors**—Lets any packets that are invalid or that encountered an error during inspection to be sent through the security appliance instead of being dropped. By default, all invalid packets or packets that failed during parsing are dropped.
- **General Parameters**—Tab that lets you configure the general parameters for the GTP inspect map.
  - **Maximum Number of Requests**—Lets you change the default for the maximum request queue size allowed. The default for the maximum request queue size is 200. Specifies the maximum number of GTP requests that will be queued waiting for a response. The permitted range is from 1 to 9999999.
  - **Maximum Number of Tunnels**—Lets you change the default for the maximum number of tunnels allowed. The default tunnel limit is 500. Specifies the maximum number of tunnels allowed. The permitted range is from 1 to 9999999 for the global overall tunnel limit.
  - **Timeouts**
    - GSN timeout**—Lets you change the default for the maximum period of inactivity before a GSN is removed. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.
    - PDP-Context timeout**—Lets you change the default for the maximum period of inactivity before receiving the PDP Context for a GTP session. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.

**Request Queue**—Lets you change the default for the maximum period of inactivity before receiving the GTP message during a GTP session. The default is 1 minute. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.

**Signaling**—Lets you change the default for the maximum period of inactivity before a GTP signaling is removed. The default is 30 minutes. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down.

**Tunnel**—Lets you change the default for the maximum period of inactivity for the GTP tunnel. The default is 1 hour. Timeout is in the format *hh:mm:ss*, where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. A value 0 means never tear down Request timeout—Specifies the GTP Request idle timeout.

**T3-Response timeout**—Specifies the maximum wait time for a response before removing the connection.

- **IMSI Prefix Filtering**—Tab that lets you configure the IMSI prefix filtering for the GTP inspect map.
  - **Mobile Country Code**—Defines the non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
  - **Mobile Network Code**—Defines the two or three-digit value identifying the network code.
  - **Add**—Add the specified country code and network code to the IMSI Prefix table.
  - **Delete**—Deletes the specified country code and network code from the IMSI Prefix table.
- **Inspections**—Tab that lets you configure the GTP inspect maps.
  - **Match Type**—Shows the match type, which can be a positive or negative match.
  - **Criterion**—Shows the criterion of the GTP inspection.
  - **Value**—Shows the value to match in the GTP inspection.
  - **Action**—Shows the action if the match condition is met.
  - **Log**—Shows the log state.
  - **Add**—Opens the Add GTP Inspect dialog box to add an GTP inspection.
  - **Edit**—Opens the Edit GTP Inspect dialog box to edit an GTP inspection.
  - **Delete**—Deletes an GTP inspection.
  - **Move Up**—Moves an inspection up in the list.
  - **Move Down**—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit GTP Map

The Add/Edit GTP Inspect dialog box lets you define the match criterion and value for the GTP inspect map.

### Fields

- **Match Type**—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- **Criterion**—Specifies which criterion of GTP traffic to match.
  - **Access Point Name**—Match on access point name.
  - **Message ID**—Match on the message ID.
  - **Message Length**—Match on the message length
  - **Version**—Match on the version.
- **Access Point Name Criterion Values**—Specifies an access point name to be matched. By default, all messages with valid APNs are inspected, and any APN is allowed.
  - **Regular Expression**—Lists the defined regular expressions to match.
  - **Manage**—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - **Regular Expression Class**—Lists the defined regular expression classes to match.
  - **Manage**—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - **Action**—Drop.
  - **Log**—Enable or disable.
- **Message ID Criterion Values**—Specifies the numeric identifier for the message that you want to match. The valid range is 1 to 255. By default, all valid message IDs are allowed.
  - **Value**—Specifies whether value is an exact match or a range.
    - Equals**—Enter a value.
    - Range**—Enter a range of values.
  - **Action**—Drop packet or limit rate (pps).
  - **Log**—Enable or disable.
- **Message Length Criterion Values**—Lets you change the default for the maximum message length for the UDP payload that is allowed.
  - **Minimum value**—Specifies the minimum number of bytes in the UDP payload. The range is from 1 to 65536.
  - **Maximum value**—Specifies the maximum number of bytes in the UDP payload. The range is from 1 to 65536.
  - **Action**—Drop packet.
  - **Log**—Enable or disable.
- **Version Criterion Values**—Specifies the GTP version for messages that you want to match. The valid range is 0-255. Use 0 to identify Version 0 and 1 to identify Version 1. Version 0 of GTP uses port 3386, while Version 1 uses port 2123. By default all GTP versions are allowed.

- Value—Specifies whether value is an exact match or a range.  
Equals—Enter a value.  
Range—Enter a range of values.
- Action—Drop packet.
- Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## H.323 Inspect Map

The H.323 pane lets you view previously configured H.323 application inspection maps. An H.323 map lets you change the default configuration values used for H.323 application inspection.

H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering and can do a cascade of inspect function activation. H.323 inspection supports phone number filtering, dynamic T.120 control, H.245 tunneling control, HSI groups, protocol state tracking, H.323 call duration enforcement, and audio/video control.

### Fields

- H.323 Inspect Maps—Table that lists the defined H.323 inspect maps.
- Add—Configures a new H.323 inspect map. To edit an H.323 inspect map, select the H.323 entry in the H.323 Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the H.323 Inspect Maps table.
- Security Level—Select the security level (low, medium, or high).
  - Low—Default.  
State Checking h225 Disabled  
State Checking ras Disabled  
Call Party Number Disabled  
Call duration Limit Disabled  
RTP conformance not enforced
  - Medium  
State Checking h225 Enabled  
State Checking ras Enabled  
Call Party Number Disabled  
Call duration Limit Disabled  
RTP conformance enforced

Limit payload to audio or video, based on the signaling exchange: no

- High

State Checking h225 Enabled

State Checking ras Enabled

Call Party Number Enabled

Call duration Limit 1:00:00

RTP conformance enforced

Limit payload to audio or video, based on the signaling exchange: yes

- Phone Number Filtering—Opens the Phone Number Filtering dialog box to configure phone number filters.
- Customize—Opens the Add/Edit H.323 Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Medium.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Phone Number Filtering

The Phone Number Filtering dialog box lets you configure the settings for a phone number filter.

### Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add Phone Number Filter dialog box to add a phone number filter.
- Edit—Opens the Edit Phone Number Filter dialog box to edit a phone number filter.
- Delete—Deletes a phone number filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit H.323 Policy Map (Security Level)

The Add/Edit H.323 Policy Map pane lets you configure the security level and additional settings for H.323 application inspection maps.

### Fields

- Name—When adding an H.323 map, enter the name of the H.323 map. When editing an H.323 map, the name of the previously configured H.323 map is shown.
- Description—Enter the description of the H.323 map, up to 200 characters in length.
- Security Level—Select the security level (low, medium, or high).
  - Low—Default.
    - State Checking h225 Disabled
    - State Checking ras Disabled
    - Call Party Number Disabled
    - Call duration Limit Disabled
    - RTP conformance not enforced
  - Medium
    - State Checking h225 Enabled
    - State Checking ras Enabled
    - Call Party Number Disabled
    - Call duration Limit Disabled
    - RTP conformance enforced
    - Limit payload to audio or video, based on the signaling exchange: no
  - High
    - State Checking h225 Enabled
    - State Checking ras Enabled
    - Call Party Number Enabled
    - Call duration Limit 1:00:00
    - RTP conformance enforced
    - Limit payload to audio or video, based on the signaling exchange: yes
  - Phone Number Filtering—Opens the Phone Number Filtering dialog box which lets you configure the settings for a phone number filter.
  - Default Level—Sets the security level back to the default.

- **Details**—Shows the State Checking, Call Attributes, Tunneling and Protocol Conformance, HSI Group Parameters, and Inspections tabs to configure additional settings.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit H.323 Policy Map (Details)

The Add/Edit H.323 Policy Map pane lets you configure the security level and additional settings for H.323 application inspection maps.

### Fields

- **Name**—When adding an H.323 map, enter the name of the H.323 map. When editing an H.323 map, the name of the previously configured H.323 map is shown.
- **Description**—Enter the description of the H.323 map, up to 200 characters in length.
- **Security Level**—Shows the security level and phone number filtering settings to configure.
- **State Checking**—Tab that lets you configure state checking parameters for the H.323 inspect map.
  - Check state transition of H.225 messages—Enforces H.323 state checking on H.225 messages.
  - Check state transition of RAS messages—Enforces H.323 state checking on RAS messages.
- **Call Attributes**—Tab that lets you configure call attributes parameters for the H.323 inspect map.
  - Enforce call duration limit—Enforces the absolute limit on a call.  
Call Duration Limit—Time limit for the call (hh:mm:ss).
  - Enforce presence of calling and called party numbers—Enforces sending call party numbers during call setup.
- **Tunneling and Protocol Conformance**—Tab that lets you configure tunneling and protocol conformance parameters for the H.323 inspect map.
  - Check for H.245 tunneling—Allows H.245 tunneling.  
Action—Drop connection or log.
  - Check RTP packets for protocol conformance—Checks RTP/RTCP packets on the pinholes for protocol conformance.  
Limit payload to audio or video, based on the signaling exchange—Enforces the payload type to be audio or video based on the signaling exchange.
- **HSI Group Parameters**—Tab that lets you configure an HSI group.
  - HSI Group ID—Shows the HSI Group ID.
  - IP Address—Shows the HSI Group IP address.
  - Endpoints—Shows the HSI Group endpoints.

- Add—Opens the Add HSI Group dialog box to add an HSI group.
- Edit—Opens the Edit HSI Group dialog box to edit an HSI group.
- Delete—Deletes an HSI group.
- Inspections—Tab that shows you the H.323 inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the H.323 inspection.
  - Value—Shows the value to match in the H.323 inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add H.323 Inspect dialog box to add an H.323 inspection.
  - Edit—Opens the Edit H.323 Inspect dialog box to edit an H.323 inspection.
  - Delete—Deletes an H.323 inspection.
  - Move Up—Moves an inspection up in the list.
  - Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HSI Group

The Add/Edit HSI Group dialog box lets you configure HSI Groups.

### Fields

- Group ID—Enter the HSI group ID.
- IP Address—Enter the HSI IP address.
- Endpoints—Lets you configure the IP address and interface of the endpoints.
  - IP Address—Enter an endpoint IP address.
  - Interface—Specifies an endpoint interface.
- Add—Adds the HSI group defined.
- Delete—Deletes the selected HSI group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit H.323 Map

The Add/Edit H.323 Inspect dialog box lets you define the match criterion and value for the H.323 inspect map.

### Fields

- **Single Match**—Specifies that the H.323 inspect has only one match statement.
- **Match Type**—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- **Criterion**—Specifies which criterion of H.323 traffic to match.
  - **Called Party**—Match the called party.
  - **Calling Party**—Match the calling party.
  - **Media Type**—Match the media type.
- **Called Party Criterion Values**—Specifies to match on the H.323 called party.
  - **Regular Expression**—Lists the defined regular expressions to match.
  - **Manage**—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - **Regular Expression Class**—Lists the defined regular expression classes to match.
  - **Manage**—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- **Calling Party Criterion Values**—Specifies to match on the H.323 calling party.
  - **Regular Expression**—Lists the defined regular expressions to match.
  - **Manage**—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - **Regular Expression Class**—Lists the defined regular expression classes to match.
  - **Manage**—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- **Media Type Criterion Values**—Specifies which media type to match.
  - **Audio**—Match audio type.
  - **Video**—Match video type.
  - **Data**—Match data type.
- **Multiple Matches**—Specifies multiple matches for the H.323 inspection.
  - **H323 Traffic Class**—Specifies the H.323 traffic class match.

- Manage—Opens the Manage H323 Class Maps dialog box to add, edit, or delete H.323 Class Maps.
- Action—Drop packet, drop connection, or reset.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## HTTP Inspect Map

The HTTP pane lets you view previously configured HTTP application inspection maps. An HTTP map lets you change the default configuration values used for HTTP application inspection.

HTTP application inspection scans HTTP headers and body, and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the security appliance.

HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.

### Fields

- HTTP Inspect Maps—Table that lists the defined HTTP inspect maps.
- Add—Configures a new HTTP inspect map. To edit an HTTP inspect map, select the HTTP entry in the HTTP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the HTTP Inspect Maps table.
- Security Level—Select the security level (low, medium, or high).
  - Low—Default.
    - Protocol violation action: Drop connection
    - Drop connections for unsafe methods: Disabled
    - Drop connections for requests with non-ASCII headers: Disabled
    - URI filtering: Not configured
    - Advanced inspections: Not configured
  - Medium
    - Protocol violation action: Drop connection
    - Drop connections for unsafe methods: Allow only GET, HEAD, and POST
    - Drop connections for requests with non-ASCII headers: Disabled
    - URI filtering: Not configured
    - Advanced inspections: Not configured

- High  
Protocol violation action: Drop connection and log  
Drop connections for unsafe methods: Allow only GET and HEAD.  
Drop connections for requests with non-ASCII headers: Enabled  
URI filtering: Not configured  
Advanced inspections: Not configured
- URI Filtering—Opens the URI Filtering dialog box to configure URI filters.
- Customize—Opens the Edit HTTP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Medium.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## URI Filtering

The URI Filtering dialog box lets you configure the settings for an URI filter.

### Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add URI Filtering dialog box to add a URI filter.
- Edit—Opens the Edit URI Filtering dialog box to edit a URI filter.
- Delete—Deletes an URI filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HTTP Policy Map (Security Level)

The Add/Edit HTTP Policy Map pane lets you configure the security level and additional settings for HTTP application inspection maps.

### Fields

- Name—When adding an HTTP map, enter the name of the HTTP map. When editing an HTTP map, the name of the previously configured HTTP map is shown.
- Description—Enter the description of the HTTP map, up to 200 characters in length.
- Security Level—Select the security level (low, medium, or high).
  - Low—Default.
    - Protocol violation action: Drop connection
    - Drop connections for unsafe methods: Disabled
    - Drop connections for requests with non-ASCII headers: Disabled
    - URI filtering: Not configured
    - Advanced inspections: Not configured
  - Medium
    - Protocol violation action: Drop connection
    - Drop connections for unsafe methods: Allow only GET, HEAD, and POST
    - Drop connections for requests with non-ASCII headers: Disabled
    - URI filtering: Not configured
    - Advanced inspections: Not configured
  - High
    - Protocol violation action: Drop connection and log
    - Drop connections for unsafe methods: Allow only GET and HEAD.
    - Drop connections for requests with non-ASCII headers: Enabled
    - URI filtering: Not configured
    - Advanced inspections: Not configured
  - URI Filtering—Opens the URI Filtering dialog box which lets you configure the settings for an URI filter.
  - Default Level—Sets the security level back to the default.
- Details—Shows the Parameters and Inspections tabs to configure additional settings.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HTTP Policy Map (Details)

The Add/Edit HTTP Policy Map pane lets you configure the security level and additional settings for HTTP application inspection maps.

**Fields**

- Name—When adding an HTTP map, enter the name of the HTTP map. When editing an HTTP map, the name of the previously configured HTTP map is shown.
- Description—Enter the description of the HTTP map, up to 200 characters in length.
- Security Level—Shows the security level and URI filtering settings to configure.
- Parameters—Tab that lets you configure the parameters for the HTTP inspect map.
  - Check for protocol violations—Checks for HTTP protocol violations.  
Action—Drop Connection, Reset, Log.  
Log—Enable or disable.
  - Spoof server string—Replaces the server HTTP header value with the specified string.  
Spoof String—Enter a string to substitute for the server header field. Maximum is 82 characters.
  - Body Match Maximum—The maximum number of characters in the body of an HTTP message that should be searched in a body match. Default is 200 bytes. A large number will have a significant impact on performance.
- Inspections—Tab that shows you the HTTP inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the HTTP inspection.
  - Value—Shows the value to match in the HTTP inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add HTTP Inspect dialog box to add an HTTP inspection.
  - Edit—Opens the Edit HTTP Inspect dialog box to edit an HTTP inspection.
  - Delete—Deletes an HTTP inspection.
  - Move Up—Moves an inspection up in the list.
  - Move Down—Moves an inspection down in the list.

**Modes**

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit HTTP Map

The Add/Edit HTTP Inspect dialog box lets you define the match criterion and value for the HTTP inspect map.

### Fields

- **Single Match**—Specifies that the HTTP inspect has only one match statement.
- **Match Type**—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- **Criterion**—Specifies which criterion of HTTP traffic to match.
  - **Request/Response Content Type Mismatch**—Specifies that the content type in the response must match one of the MIME types in the accept field of the request.
  - **Request Arguments**—Applies the regular expression match to the arguments of the request.  
Regular Expression—Lists the defined regular expressions to match.  
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
Regular Expression Class—Lists the defined regular expression classes to match.  
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - **Request Body Length**—Applies the regular expression match to the body of the request with field length greater than the bytes specified.  
Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.
  - **Request Body**—Applies the regular expression match to the body of the request.  
Regular Expression—Lists the defined regular expressions to match.  
Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.  
Regular Expression Class—Lists the defined regular expression classes to match.  
Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
  - **Request Header Field Count**—Applies the regular expression match to the header of the request with a maximum number of header fields.  
Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type,

cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Request Header Field Length—Applies the regular expression match to the header of the request with field length greater than the bytes specified.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that request field lengths will be matched against.

- Request Header Field—Applies the regular expression match to the header of the request.

Predefined—Specifies the request header fields: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request Header Count—Applies the regular expression match to the header of the request with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Request Header Length—Applies the regular expression match to the header of the request with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Request Header non-ASCII—Matches non-ASCII characters in the header of the request.
- Request Method—Applies the regular expression match to the method of the request.

Method—Specifies to match on a request method: bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.

Regular Expression—Specifies to match on a regular expression.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Request URI Length—Applies the regular expression match to the URI of the request with length greater than the bytes specified.

Greater Than Length—Enter a URI length value in bytes.

- Request URI—Applies the regular expression match to the URI of the request.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Body—Applies the regex match to the body of the response.

ActiveX—Specifies to match on ActiveX.

Java Applet—Specifies to match on a Java Applet.

Regular Expression—Specifies to match on a regular expression.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Body Length—Applies the regular expression match to the body of the response with field length greater than the bytes specified.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field Count—Applies the regular expression match to the header of the response with a maximum number of header fields.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Count—Enter the maximum number of header fields.

- Response Header Field Length—Applies the regular expression match to the header of the response with field length greater than the bytes specified.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Greater Than Length—Enter a field length value in bytes that response field lengths will be matched against.

- Response Header Field—Applies the regular expression match to the header of the response.

Predefined—Specifies the response header fields: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Response Header Count—Applies the regular expression match to the header of the response with a maximum number of headers.

Greater Than Count—Enter the maximum number of headers.

- Response Header Length—Applies the regular expression match to the header of the response with length greater than the bytes specified.

Greater Than Length—Enter a header length value in bytes.

- Response Header non-ASCII—Matches non-ASCII characters in the header of the response.
- Response Status Line—Applies the regular expression match to the status line.

Regular Expression—Lists the defined regular expressions to match.

Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

Regular Expression Class—Lists the defined regular expression classes to match.

Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.

- Multiple Matches—Specifies multiple matches for the HTTP inspection.

- H323 Traffic Class—Specifies the HTTP traffic class match.
- Manage—Opens the Manage HTTP Class Maps dialog box to add, edit, or delete HTTP Class Maps.
- Action—Drop connection, reset, or log.
- Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Instant Messaging (IM) Inspect Map

The IM pane lets you view previously configured Instant Messaging (IM) application inspection maps. An Instant Messaging (IM) map lets you change the default configuration values used for Instant Messaging (IM) application inspection.

Instant Messaging (IM) application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and propagations of network threats. A regular expression database search representing various patterns for Instant Messaging (IM) protocols to be filtered is applied. A syslog is generated if the flow is not recognized.

The scope can be limited by using an access list to specify any traffic streams to be inspected. For UDP messages, a corresponding UDP port number is also configurable. Inspection of Yahoo! Messenger and MSN Messenger instant messages are supported.

### Fields

- Name—Enter the name of the inspect map, up to 40 characters in length.
- Description—Enter the description of the inspect map, up to 200 characters in length.
- IM Inspect Maps—Table that lists the defined IM inspect maps.
- Add—Configures a new IM inspect map.
- Edit—Edits the selected IM entry in the IM Inspect Maps table.
- Delete—Deletes the inspect map selected in the IM Inspect Maps table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Instant Messaging (IM) Policy Map

The Add/Edit Instant Messaging (IM) Policy Map pane lets you configure the security level and additional settings for IM application inspection maps.

### Fields

- **Name**—When adding an IM map, enter the name of the IM map. When editing an IM map, the name of the previously configured IM map is shown.
- **Description**—Enter the description of the IM map, up to 200 characters in length.
- **Match Type**—Shows the match type, which can be a positive or negative match.
- **Criterion**—Shows the criterion of the IM inspection.
- **Value**—Shows the value to match in the IM inspection.
- **Action**—Shows the action if the match condition is met.
- **Log**—Shows the log state.
- **Add**—Opens the Add IM Inspect dialog box to add an IM inspection.
- **Edit**—Opens the Edit IM Inspect dialog box to edit an IM inspection.
- **Delete**—Deletes an IM inspection.
- **Move Up**—Moves an inspection up in the list.
- **Move Down**—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IM Map

The Add/Edit IM Inspect dialog box lets you define the match criterion and value for the IM inspect map.

### Fields

- **Single Match**—Specifies that the IM inspect has only one match statement.
- **Match Type**—Specifies whether traffic should match or not match the values.

For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

- **Criterion**—Specifies which criterion of IM traffic to match.
  - **Protocol**—Match IM protocols.
  - **Service**—Match IM services.
  - **Source IP Address**—Match source IP address.

- Destination IP Address—Match destination IP address.
  - Version—Match IM file transfer service version.
  - Client Login Name—Match client login name from IM service.
  - Client Peer Login Name—Match client peer login name from IM service.
  - Filename—Match filename from IM file transfer service.
- Protocol Criterion Values—Specifies which IM protocols to match.
  - Yahoo! Messenger—Specifies to match Yahoo! Messenger instant messages.
  - MSN Messenger—Specifies to match MSN Messenger instant messages.
- Service Criterion Values—Specifies which IM services to match.
  - Chat—Specifies to match IM message chat service.
  - Conference—Specifies to match IM conference service.
  - File Transfer—Specifies to match IM file transfer service.
  - Games—Specifies to match IM gaming service.
  - Voice Chat—Specifies to match IM voice chat service (not available for Yahoo IM)
  - Web Cam—Specifies to match IM webcam service.
- Source IP Address Criterion Values—Specifies to match the source IP address of the IM service.
  - IP Address—Enter the source IP address of the IM service.
  - IP Mask—Mask of the source IP address.
- Destination IP Address Criterion Values—Specifies to match the destination IP address of the IM service.
  - IP Address—Enter the destination IP address of the IM service.
  - IP Mask—Mask of the destination IP address.
- Version Criterion Values—Specifies to match the version from the IM file transfer service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Login Name Criterion Values—Specifies to match the client login name from the IM service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Client Peer Login Name Criterion Values—Specifies to match the client peer login name from the IM service. Applies the regular expression match.

- Regular Expression—Lists the defined regular expressions to match.
- Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Filename Criterion Values—Specifies to match the filename from the IM file transfer service. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Multiple Matches—Specifies multiple matches for the IM inspection.
  - IM Traffic Class—Specifies the IM traffic class match.
  - Manage—Opens the Manage IM Class Maps dialog box to add, edit, or delete IM Class Maps.
- Action—Drop connection, reset, or log.
- Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## IPSec Pass Through Inspect Map

The IPSec Pass Through pane lets you view previously configured IPSec Pass Through application inspection maps. An IPSec Pass Through map lets you change the default configuration values used for IPSec Pass Through application inspection. You can use an IPSec Pass Through map to permit certain flows without using an access list.

### Fields

- IPSec Pass Through Inspect Maps—Table that lists the defined IPSec Pass Through inspect maps.
- Add—Configures a new IPSec Pass Through inspect map. To edit an IPSec Pass Through inspect map, select the IPSec Pass Through entry in the IPSec Pass Through Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the IPSec Pass Through Inspect Maps table.
- Security Level—Select the security level (high or low).



- Low—Default.  
Maximum ESP flows per client: Unlimited.  
ESP idle timeout: 00:10:00.  
Maximum AH flows per client: Unlimited.  
AH idle timeout: 00:10:00.
- High  
Maximum ESP flows per client: 10.  
ESP idle timeout: 00:00:30.  
Maximum AH flows per client: 10.  
AH idle timeout: 00:00:30.
- Customize—Opens the Add/Edit IPSec Pass Thru Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IPSec Pass Thru Policy Map (Security Level)

The Add/Edit IPSec Pass Thru Policy Map pane lets you configure the security level and additional settings for IPSec Pass Thru application inspection maps.

### Fields

- Name—When adding an IPSec Pass Thru map, enter the name of the IPSec Pass Thru map. When editing an IPSec Pass Thru map, the name of the previously configured IPSec Pass Thru map is shown.
- Security Level—Select the security level (high or low).
  - Low—Default.  
Maximum ESP flows per client: Unlimited.  
ESP idle timeout: 00:10:00.  
Maximum AH flows per client: Unlimited.  
AH idle timeout: 00:10:00.
  - High  
Maximum ESP flows per client: 10.  
ESP idle timeout: 00:00:30.  
Maximum AH flows per client: 10.

AH idle timeout: 00:00:30.

- Default Level—Sets the security level back to the default level of Low.
- Details—Shows additional parameter settings to configure.

### Mode

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IPSec Pass Thru Policy Map (Details)

The Add/Edit IPSec Pass Thru Policy Map pane lets you configure the security level and additional settings for IPSec Pass Thru application inspection maps.

### Fields

- Name—When adding an IPSec Pass Thru map, enter the name of the IPSec Pass Thru map. When editing an IPSec Pass Thru map, the name of the previously configured IPSec Pass Thru map is shown.
- Description—Enter the description of the IPSec Pass Through map, up to 200 characters in length.
- Security Level—Shows the security level settings to configure.
- Parameters—Configures ESP and AH parameter settings.
  - Limit ESP flows per client—Limits ESP flows per client.  
Maximum—Specify maximum limit.
  - Apply ESP idle timeout—Applies ESP idle timeout.  
Timeout—Specify timeout.
  - Limit AH flows per client—Limits AH flows per client.  
Maximum—Specify maximum limit.
  - Apply AH idle timeout—Applies AH idle timeout.  
Timeout—Specify timeout.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## MGCP Inspect Map

The MGCP pane lets you view previously configured MGCP application inspection maps. An MGCP map lets you change the default configuration values used for MGCP application inspection. You can use an MGCP map to manage connections between VoIP devices and MGCP call agents.

### Fields

- **MGCP Inspect Maps**—Table that lists the defined MGCP inspect maps.
- **Add**—Configures a new MGCP inspect map.
- **Edit**—Edits the selected MGCP entry in the MGCP Inspect Maps table.
- **Delete**—Deletes the inspect map selected in the MGCP Inspect Maps table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Gateways and Call Agents

The Gateways and Call Agents dialog box lets you configure groups of gateways and call agents for the map.

### Fields

- **Group ID**—Identifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The gateway IP address can only be associated with one group ID. You cannot use the same gateway with different group IDs. The valid range is from 0 to 2147483647.
- **Criterion**—Shows the criterion of the inspection.
- **Gateways**—Identifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
- **Call Agents**—Identifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
- **Add**—Displays the Add MGCP dialog box, which you can use to define a new application inspection map.
- **Edit**—Displays the Edit MGCP dialog box, which you can use to modify the application inspection map selected in the application inspection map table.
- **Delete**—Deletes the application inspection map selected in the application inspection map table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit MGCP Policy Map

The Add/Edit MGCP Policy Map pane lets you configure the command queue, gateway, and call agent settings for MGCP application inspection maps.

### Fields

- Name—When adding an MGCP map, enter the name of the MGCP map. When editing an MGCP map, the name of the previously configured MGCP map is shown.
- Description—Enter the description of the MGCP map, up to 200 characters in length.
- Command Queue—Tab that lets you specify the permitted queue size for MGCP commands.
  - Command Queue Size—Specifies the maximum number of commands to queue. The valid range is from 1 to 2147483647.
- Gateways and Call Agents—Tab that lets you configure groups of gateways and call agents for this map.
  - Group ID—Identifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The gateway IP address can only be associated with one group ID. You cannot use the same gateway with different group IDs. The valid range is from 0 to 2147483647.
  - Criterion—Shows the criterion of the inspection.
  - Gateways—Identifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
  - Call Agents—Identifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
  - Add—Displays the Add MGCP Group dialog box, which you can use to define a new MGCP group of gateways and call agents.
  - Edit—Displays the Edit MGCP dialog box, which you can use to modify the MGCP group selected in the Gateways and Call Agents table.
  - Delete—Deletes the MGCP group selected in the Gateways and Call Agents table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit MGCP Group

The Add/Edit MGCP Group dialog box lets you define the configuration of an MGCP group that will be used when MGCP application inspection is enabled.

### Fields

- Group ID—Specifies the ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The valid range is from 0 to 2147483647.
- Gateways area
  - Gateway to Be Added—Specifies the IP address of the media gateway that is controlled by the associated call agent. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, 2727.
  - Add—Adds the specified IP address to the IP address table.
  - Delete—Deletes the selected IP address from the IP address table.
  - IP Address—Lists the IP addresses of the gateways in the call agent group.
- Call Agents
  - Call Agent to Be Added—Specifies the IP address of a call agent that controls the MGCP media gateways in the call agent group. Normally, a call agent sends commands to the default MGCP port for gateways, 2427.
  - Add—Adds the specified IP address to the IP address table.
  - Delete—Deletes the selected IP address from the IP address table.
  - IP Address—Lists the IP addresses of the call agents in the call agent group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## NetBIOS Inspect Map

The NetBIOS pane lets you view previously configured NetBIOS application inspection maps. A NetBIOS map lets you change the default configuration values used for NetBIOS application inspection.

NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.

### Fields

- NetBIOS Inspect Maps—Table that lists the defined NetBIOS inspect maps.
- Add—Configures a new NetBIOS inspect map.
- Edit—Edits the selected NetBIOS entry in the NetBIOS Inspect Maps table.
- Delete—Deletes the inspect map selected in the NetBIOS Inspect Maps table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit NetBIOS Policy Map

The Add/Edit NetBIOS Policy Map pane lets you configure the protocol violation settings for NetBIOS application inspection maps.

### Fields

- Name—When adding a NetBIOS map, enter the name of the NetBIOS map. When editing an NetBIOS map, the name of the previously configured NetBIOS map is shown.
- Description—Enter the description of the NetBIOS map, up to 200 characters in length.
- Check for protocol violations—Checks for protocol violations and executes specified action.
  - Action—Drop packet or log.
  - Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## RTSP Inspect Map

The RTSP pane lets you view previously configured RTSP application inspection maps. An RTSP map lets you change the default configuration values used for RTSP application inspection. You can use an RTSP map to protect RTSP traffic.

### Fields

- RTSP Inspect Maps—Table that lists the defined RTSP inspect maps.
- Add—Configures a new RTSP inspect map.
- Edit—Edits the selected RTSP entry in the RTSP Inspect Maps table.
- Delete—Deletes the inspect map selected in the RTSP Inspect Maps table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit RTSP Policy Map

The Add/Edit RTSP Policy Map pane lets you configure the parameters and inspections settings for RTSP application inspection maps.

### Fields

- Name—When adding an RTSP map, enter the name of the RTSP map. When editing an RTSP map, the name of the previously configured RTSP map is shown.
- Description—Enter the description of the RTSP map, up to 200 characters in length.
- Parameters—Tab that lets you restrict usage on reserved ports during media port negotiation, and lets you set the URL length limit.
  - Enforce Reserve Port Protection—Lets you restrict the use of reserved ports during media port negotiation.
  - Maximum URL Length—Specifies the maximum length of the URL allowed in the message. Maximum value is 6000.
- Inspections—Tab that shows you the RTSP inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the RTSP inspection.
  - Value—Shows the value to match in the RTSP inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add RTSP Inspect dialog box to add a RTSP inspection.

- Edit—Opens the Edit RTSP Inspect dialog box to edit a RTSP inspection.
- Delete—Deletes a RTSP inspection.
- Move Up—Moves an inspection up in the list.
- Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit RTSP Inspect

The Add/Edit RTSP Inspect dialog box lets you define the match criterion, values, and actions for the RTSP inspect map.

### Fields

- Match Type—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of RTSP traffic to match.
  - URL Filter—Match URL filtering.
  - Request Method—Match an RTSP request method.
- URL Filter Criterion Values—Specifies to match URL filtering. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URL Filter Actions—Primary action and log settings.
  - Action—Drop connection or log.
  - Log—Enable or disable.
- Request Method Criterion Values—Specifies to match an RTSP request method.
  - Request Method—Specifies a request method: announce, describe, get\_parameter, options, pause, play, record, redirect, setup, set\_parameters, teardown.
- Request Method Actions—Primary action settings.
  - Action—Limit rate (pps).



### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SCCP (Skinny) Inspect Map

The SCCP (Skinny) pane lets you view previously configured SCCP (Skinny) application inspection maps. An SCCP (Skinny) map lets you change the default configuration values used for SCCP (Skinny) application inspection.

Skinny application inspection performs translation of embedded IP address and port numbers within the packet data, and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.

### Fields

- SCCP (Skinny) Inspect Maps—Table that lists the defined SCCP (Skinny) inspect maps.
- Add—Configures a new SCCP (Skinny) inspect map. To edit an SCCP (Skinny) inspect map, select the SCCP (Skinny) entry in the SCCP (Skinny) Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the SCCP (Skinny) Inspect Maps table.
- Security Level—Select the security level (high or low).
  - Low—Default.
    - Registration: Not enforced.
    - Maximum message ID: 0x181.
    - Minimum prefix length: 4
    - Media timeout: 00:05:00
    - Signaling timeout: 01:00:00.
    - RTP conformance: Not enforced.
  - Medium
    - Registration: Not enforced.
    - Maximum message ID: 0x141.
    - Minimum prefix length: 4.
    - Media timeout: 00:01:00.
    - Signaling timeout: 00:05:00.
    - RTP conformance: Enforced.
    - Limit payload to audio or video, based on the signaling exchange: No.
  - High
    - Registration: Enforced.

Maximum message ID: 0x141.

Minimum prefix length: 4.

Maximum prefix length: 65536.

Media timeout: 00:01:00.

Signaling timeout: 00:05:00.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: Yes.

- Message ID Filtering—Opens the Messaging ID Filtering dialog box for configuring message ID filters.
- Customize—Opens the Add/Edit SCCP (Skinny) Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Message ID Filtering

The Message ID Filtering dialog box lets you configure the settings for a message ID filter.

### Fields

- Match Type—Shows the match type, which can be a positive or negative match.
- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add Message ID Filtering dialog box to add a message ID filter.
- Edit—Opens the Edit Message ID Filtering dialog box to edit a message ID filter.
- Delete—Deletes a message ID filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SCCP (Skinny) Policy Map (Security Level)

The Add/Edit SCCP (Skinny) Policy Map pane lets you configure the security level and additional settings for SCCP (Skinny) application inspection maps.

### Fields

- Name—When adding an SCCP (Skinny) map, enter the name of the SCCP (Skinny) map. When editing an SCCP (Skinny) map, the name of the previously configured SCCP (Skinny) map is shown.
- Description—Enter the description of the SCCP (Skinny) map, up to 200 characters in length.
- Security Level—Select the security level (high or low).
  - Low—Default.
    - Registration: Not enforced.
    - Maximum message ID: 0x181.
    - Minimum prefix length: 4
    - Media timeout: 00:05:00
    - Signaling timeout: 01:00:00.
    - RTP conformance: Not enforced.
  - Medium
    - Registration: Not enforced.
    - Maximum message ID: 0x141.
    - Minimum prefix length: 4.
    - Media timeout: 00:01:00.
    - Signaling timeout: 00:05:00.
    - RTP conformance: Enforced.
    - Limit payload to audio or video, based on the signaling exchange: No.
  - High
    - Registration: Enforced.
    - Maximum message ID: 0x141.
    - Minimum prefix length: 4.
    - Maximum prefix length: 65536.
    - Media timeout: 00:01:00.
    - Signaling timeout: 00:05:00.
    - RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: Yes.

- Message ID Filtering—Opens the Messaging ID Filtering dialog box for configuring message ID filters.
- Default Level—Sets the security level back to the default.
- Details—Shows additional parameter, RTP conformance, and message ID filtering settings to configure.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SCCP (Skinny) Policy Map (Details)

The Add/Edit SCCP (Skinny) Policy Map pane lets you configure the security level and additional settings for SCCP (Skinny) application inspection maps.

### Fields

- Name—When adding an SCCP (Skinny) map, enter the name of the SCCP (Skinny) map. When editing an SCCP (Skinny) map, the name of the previously configured SCCP (Skinny) map is shown.
- Description—Enter the description of the DNS map, up to 200 characters in length.
- Security Level—Shows the security level and message ID filtering settings to configure.
- Parameters—Tab that lets you configure the parameter settings for SCCP (Skinny).
  - Enforce endpoint registration—Enforce that Skinny endpoints are registered before placing or receiving calls.
    - Maximum Message ID—Specify value of maximum SCCP message ID allowed.
  - SCCP Prefix Length—Specifies prefix length value in Skinny messages.
    - Minimum Prefix Length—Specify minimum value of SCCP prefix length allowed.
    - Maximum Prefix Length—Specify maximum value of SCCP prefix length allowed.
  - Media Timeout—Specify timeout value for media connections.
  - Signaling Timeout—Specify timeout value for signaling connections.
- RTP Conformance—Tab that lets you configure the RTP conformance settings for SCCP (Skinny).
  - Check RTP packets for protocol conformance—Checks RTP/RTCP packets flowing on the pinholes for protocol conformance.
    - Limit payload to audio or video, based on the signaling exchange—Enforces the payload type to be audio/video based on the signaling exchange.
- Message ID Filtering—Tab that lets you configure the message ID filtering settings for SCCP (Skinny).
  - Match Type—Shows the match type, which can be a positive or negative match.

- Criterion—Shows the criterion of the inspection.
- Value—Shows the value to match in the inspection.
- Action—Shows the action if the match condition is met.
- Log—Shows the log state.
- Add—Opens the Add Message ID Filtering dialog box to add a message ID filter.
- Edit—Opens the Edit Message ID Filtering dialog box to edit a message ID filter.
- Delete—Deletes a message ID filter.
- Move Up—Moves an entry up in the list.
- Move Down—Moves an entry down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Message ID Filter

The Add Message ID Filter dialog box lets you configure message ID filters.

### Fields

- Match Type—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of SCCP (Skinny) traffic to match.
  - Message ID—Match specified message ID.  
Message ID—Specify value of maximum SCCP message ID allowed.
  - Message ID Range—Match specified message ID range.  
Lower Message ID—Specify lower value of SCCP message ID allowed.  
Upper Message ID—Specify upper value of SCCP message ID allowed.
- Action—Drop packet.
- Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SIP Inspect Map

The SIP pane lets you view previously configured SIP application inspection maps. A SIP map lets you change the default configuration values used for SIP application inspection.

SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.

SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks. It also supports application security and protocol conformance, which enforce the sanity of the SIP messages, as well as detect SIP-based attacks.

### Fields

- SIP Inspect Maps—Table that lists the defined SIP inspect maps.
- Add—Configures a new SIP inspect map. To edit a SIP inspect map, select the SIP entry in the SIP Inspect Maps table and click Customize.
- Delete—Deletes the inspect map selected in the SIP Inspect Maps table.
- Security Level—Select the security level (high or low).
  - Low—Default.
    - SIP instant messaging (IM) extensions: Enabled.
    - Non-SIP traffic on SIP port: Permitted.
    - Hide server's and endpoint's IP addresses: Disabled.
    - Mask software version and non-SIP URIs: Disabled.
    - Ensure that the number of hops to destination is greater than 0: Enabled.
    - RTP conformance: Not enforced.
    - SIP conformance: Do not perform state checking and header validation.
  - Medium
    - SIP instant messaging (IM) extensions: Enabled.
    - Non-SIP traffic on SIP port: Permitted.
    - Hide server's and endpoint's IP addresses: Disabled.
    - Mask software version and non-SIP URIs: Disabled.
    - Ensure that the number of hops to destination is greater than 0: Enabled.
    - RTP conformance: Enforced.
    - Limit payload to audio or video, based on the signaling exchange: No
    - SIP conformance: Drop packets that fail state checking.

- High
  - SIP instant messaging (IM) extensions: Enabled.
  - Non-SIP traffic on SIP port: Denied.
  - Hide server's and endpoint's IP addresses: Disabled.
  - Mask software version and non-SIP URIs: Enabled.
  - Ensure that the number of hops to destination is greater than 0: Enabled.
  - RTP conformance: Enforced.
  - Limit payload to audio or video, based on the signaling exchange: Yes
  - SIP conformance: Drop packets that fail state checking and packets that fail header validation.
- Customize—Opens the Add/Edit SIP Policy Map dialog box for additional settings.
- Default Level—Sets the security level back to the default level of Low.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SIP Policy Map (Security Level)

The Add/Edit SIP Policy Map pane lets you configure the security level and additional settings for SIP application inspection maps.

### Fields

- Name—When adding a SIP, enter the name of the SIP map. When editing a SIP map, the name of the previously configured SIP map is shown.
- Description—Enter the description of the SIP map, up to 200 characters in length.
- Security Level—Select the security level (high or low).
  - Low—Default.
    - SIP instant messaging (IM) extensions: Enabled.
    - Non-SIP traffic on SIP port: Permitted.
    - Hide server's and endpoint's IP addresses: Disabled.
    - Mask software version and non-SIP URIs: Disabled.
    - Ensure that the number of hops to destination is greater than 0: Enabled.
    - RTP conformance: Not enforced.
    - SIP conformance: Do not perform state checking and header validation.
  - Medium
    - SIP instant messaging (IM) extensions: Enabled.

Non-SIP traffic on SIP port: Permitted.

Hide server's and endpoint's IP addresses: Disabled.

Mask software version and non-SIP URIs: Disabled.

Ensure that the number of hops to destination is greater than 0: Enabled.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: No

SIP conformance: Drop packets that fail state checking.

– High

SIP instant messaging (IM) extensions: Enabled.

Non-SIP traffic on SIP port: Denied.

Hide server's and endpoint's IP addresses: Disabled.

Mask software version and non-SIP URIs: Enabled.

Ensure that the number of hops to destination is greater than 0: Enabled.

RTP conformance: Enforced.

Limit payload to audio or video, based on the signaling exchange: Yes

SIP conformance: Drop packets that fail state checking and packets that fail header validation.

– Default Level—Sets the security level back to the default.

- Details—Shows additional filtering, IP address privacy, hop count, RTP conformance, SIP conformance, field masking, and inspections settings to configure.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SIP Policy Map (Details)

The Add/Edit SIP Policy Map pane lets you configure the security level and additional settings for SIP application inspection maps.

### Fields

- Name—When adding a SIP, enter the name of the SIP map. When editing a SIP map, the name of the previously configured SIP map is shown.
- Description—Enter the description of the SIP map, up to 200 characters in length.
- Security Level—Shows the security level settings to configure
- Filtering—Tab that lets you configure the filtering settings for SIP.



- Enable SIP instant messaging (IM) extensions—Enables Instant Messaging extensions. Default is enabled.
  - Permit non-SIP traffic on SIP port—Permits non-SIP traffic on SIP port. Permitted by default.
- IP Address Privacy—Tab that lets you configure the IP address privacy settings for SIP.
  - Hide server's and endpoint's IP addresses—Enables IP address privacy. Disabled by default.
- Hop Count—Tab that lets you configure the hop count settings for SIP.
  - Ensure that number of hops to destination is greater than 0—Enables check for the value of Max-Forwards header is zero.  
Action—Drop packet, Drop Connection, Reset, Log.  
Log—Enable or Disable.
- RTP Conformance—Tab that lets you configure the RTP conformance settings for SIP.
  - Check RTP packets for protocol conformance—Checks RTP/RTCP packets flowing on the pinholes for protocol conformance.  
Limit payload to audio or video, based on the signaling exchange—Enforces payload type to be audio/video based on the signaling exchange.
- SIP Conformance—Tab that lets you configure the SIP conformance settings for SIP.
  - Enable state transition checking—Enables SIP state checking.  
Action—Drop packet, Drop Connection, Reset, Log.  
Log—Enable or Disable.
  - Enable strict validation of header fields—Enables validation of SIP header fields.  
Action—Drop packet, Drop Connection, Reset, Log.  
Log—Enable or Disable.
- Field Masking—Tab that lets you configure the field masking settings for SIP.
  - Inspect non-SIP URIs—Enables non-SIP URI inspection in Alert-Info and Call-Info headers.  
Action—Mask or Log.  
Log—Enable or Disable.
  - Inspect server's and endpoint's software version—Inspects SIP endpoint software version in User-Agent and Server headers.  
Action—Mask or Log.  
Log—Enable or Disable.
- Inspections—Tab that shows you the SIP inspection configuration and lets you add or edit.
  - Match Type—Shows the match type, which can be a positive or negative match.
  - Criterion—Shows the criterion of the SIP inspection.
  - Value—Shows the value to match in the SIP inspection.
  - Action—Shows the action if the match condition is met.
  - Log—Shows the log state.
  - Add—Opens the Add SIP Inspect dialog box to add a SIP inspection.
  - Edit—Opens the Edit SIP Inspect dialog box to edit a SIP inspection.
  - Delete—Deletes a SIP inspection.

- Move Up—Moves an inspection up in the list.
- Move Down—Moves an inspection down in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SIP Inspect

The Add/Edit SIP Inspect dialog box lets you define the match criterion and value for the SIP inspect map.

### Fields

- Single Match—Specifies that the SIP inspect has only one match statement.
- Match Type—Specifies whether traffic should match or not match the values.  
For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
- Criterion—Specifies which criterion of SIP traffic to match.
  - Called Party—Match a called party as specified in the To header.
  - Calling Party—Match a calling party as specified in the From header.
  - Content Length—Match a content length header.
  - Content Type—Match a content type header.
  - IM Subscriber—Match a SIP IM subscriber.
  - Message Path—Match a SIP Via header.
  - Request Method—Match a SIP request method.
  - Third-Party Registration—Match the requester of a third-party registration.
  - URI Length—Match a URI in the SIP headers.
- Called Party Criterion Values—Specifies to match the called party. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Calling Party Criterion Values—Specifies to match the calling party. Applies the regular expression match.

- Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Content Length Criterion Values—Specifies to match a SIP content header of a length greater than specified.
  - Greater Than Length—Enter a header length value in bytes.
- Content Type Criterion Values—Specifies to match a SIP content header type.
  - SDP—Match an SDP SIP content header type.
  - Regular Expression—Match a regular expression.
    - Regular Expression—Lists the defined regular expressions to match.
    - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
    - Regular Expression Class—Lists the defined regular expression classes to match.
    - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- IM Subscriber Criterion Values—Specifies to match the IM subscriber. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Message Path Criterion Values—Specifies to match a SIP Via header. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.
  - Regular Expression Class—Lists the defined regular expression classes to match.
  - Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- Request Method Criterion Values—Specifies to match a SIP request method.
  - Request Method—Specifies a request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- Third-Party Registration Criterion Values—Specifies to match the requester of a third-party registration. Applies the regular expression match.
  - Regular Expression—Lists the defined regular expressions to match.
  - Manage—Opens the Manage Regular Expressions dialog box, which lets you configure regular expressions.

- Regular Expression Class—Lists the defined regular expression classes to match.
- Manage—Opens the Manage Regular Expression Class dialog box, which lets you configure regular expression class maps.
- URI Length Criterion Values—Specifies to match a URI in the SIP headers greater than specified length.
  - URI type—Specifies to match either SIP URI or TEL URI.
  - Greater Than Length—Length in bytes.
- Multiple Matches—Specifies multiple matches for the SIP inspection.
  - SIP Traffic Class—Specifies the SIP traffic class match.
  - Manage—Opens the Manage SIP Class Maps dialog box to add, edit, or delete SIP Class Maps.
- Actions—Primary action and log settings.
  - Action—Drop packet, drop connection, reset, log. Note: Limit rate (pps) action is available for request methods invite and register.
  - Log—Enable or disable.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SNMP Inspect Map

The SNMP pane lets you view previously configured SNMP application inspection maps. An SNMP map lets you change the default configuration values used for SNMP application inspection.

### Fields

- Map Name—Lists previously configured application inspection maps. Check a map and click **Edit** to view or change an existing map.
- Add—Configures a new SNMP inspect map.
- Edit—Edits the selected SNMP entry in the SNMP Inspect Maps table.
- Delete—Deletes the inspect map selected in the SNMP Inspect Maps table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit SNMP Map

The Add/Edit SNMP Map dialog box lets you create a new SNMP map for controlling SNMP application inspection.

### Fields

- SNMP Map Name—Defines the name of the application inspection map.
- SNMP version 1—Enables application inspection for SNMP version 1.
- SNMP version 2 (party based)—Enables application inspection for SNMP version 2.
- SNMP version 2c (community based)—Enables application inspection for SNMP version 2c.
- SNMP version 3—Enables application inspection for SNMP version 3.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |





# CHAPTER 25

## Configuring QoS

---

Have you ever participated in a long-distance phone call that involved a satellite connection? The conversation might be interrupted with brief, but perceptible, gaps at odd intervals. Those gaps are the time, called the latency, between the arrival of packets being transmitted over the network. Some network traffic, such as voice and video, cannot tolerate long latency times. Quality of Service (QoS) is a feature that lets you give priority to critical traffic, prevent bandwidth hogging, and manage network bottlenecks to prevent packet drops.

This chapter describes how to apply QoS policies, and includes the following sections:

- [QoS Overview, page 25-1](#)
- [Creating the Standard Priority Queue for an Interface, page 25-5](#)
- [Creating a Policy for Standard Priority Queueing and/or Policing, page 25-6](#)
- [Creating a Policy for Traffic Shaping and Hierarchical Priority Queueing, page 25-7](#)

## QoS Overview

You should consider that in an ever-changing network environment, QoS is not a one-time deployment, but an ongoing, essential part of network design.



### Note

---

QoS is only available in single context mode.

---

This section describes the QoS features supported by the security appliance, and includes the following topics:

- [Supported QoS Features, page 25-2](#)
- [What is a Token Bucket?, page 25-2](#)
- [Policing Overview, page 25-3](#)
- [Priority Queueing Overview, page 25-3](#)
- [Traffic Shaping Overview, page 25-4](#)
- [DSCP and DiffServ Preservation, page 25-5](#)

## Supported QoS Features

The security appliance supports the following QoS features:

- **Policing**—To prevent individual flows from hogging the network bandwidth, you can limit the maximum bandwidth used per flow. See the [“Policing Overview” section on page 25-3](#) for more information.
- **Priority queuing**—For critical traffic that cannot tolerate latency, such as Voice over IP (VoIP), you can identify traffic for Low Latency Queuing (LLQ) so that it is always transmitted ahead of other traffic. See the [“Priority Queueing Overview” section on page 25-3](#) for more information.
- **Traffic shaping**—If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the [“Traffic Shaping Overview” section on page 25-4](#) for more information.

## What is a Token Bucket?

A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic policer or a traffic shaper. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator.

A token bucket is a formal definition of a rate of transfer. It has three components: a burst size, an average rate, and a time interval. Although the average rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

average rate = burst size / time interval

These terms are defined as follows:

- **Average rate**—Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.
- **Burst size**—Also called the Committed Burst (Bc) size, it specifies in bits or bytes per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For traffic shaping, it specifies bits per burst; for policing, it specifies bytes per burst.)
- **Time interval**—Also called the measurement interval, it specifies the time quantum in seconds per burst.

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet either waits until the bucket has enough tokens (in the case of traffic shaping) or the packet is discarded or marked down (in the case of policing). If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. Thus, at any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

Note that the token bucket mechanism used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a policer. For traffic shaping, packets that arrive that cannot be sent immediately are delayed in the data buffer.



For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the token bucket capacity, divided by the time interval, plus the established rate at which tokens are placed in the token bucket. See the following formula:

$$(\text{token bucket capacity in bits} / \text{time interval in seconds}) + \text{established rate in bps} = \text{maximum flow speed in bps}$$

This method of bounding burstiness also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

## Policing Overview

Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow or class can take over the entire resource. When traffic exceeds the maximum rate, the security appliance drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

## Priority Queueing Overview

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface (see the [“Creating the Standard Priority Queue for an Interface”](#) section on page 25-5), while all other traffic goes into the “best effort” queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queueing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queueing:
  - Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.
  - Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
  - For IPSec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
  - IPSec-over-TCP is not supported for priority traffic classification.

## Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPSec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the Burst Size value. See the [“What is a Token Bucket?”](#) section on page 25-2.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queueing, see the [“Priority Queueing Overview”](#) section on page 25-3):
  - The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
  - When the queue limit is reached, packets are tail-dropped.
  - Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
  - The time interval is derived by  $time\_interval = burst\_size / average\_rate$ . The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

Average Rate = 1000000

Burst Size = 1000000

In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

## How QoS Features Interact

You can configure each of the QoS features alone if desired for the security appliance. Often, though, you configure multiple QoS features on the security appliance so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).  
You cannot configure priority queueing and policing for the same set of traffic.
- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

You cannot configure traffic shaping and standard priority queueing for the same interface; only hierarchical priority queueing is allowed. For example, if you configure standard priority queueing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the security appliance does not restrict you from configuring this.

## DSCP and DiffServ Preservation

- DSCP markings are preserved on all traffic passing through the security appliance.
- The security appliance does not locally mark/re-mark any classified traffic, but it honors the Expedited Forwarding (EF) DSCP bits of every packet to determine if it requires “priority” handling and will direct those packets to the LLQ.
- DiffServ marking is preserved on packets when they traverse the service provider backbone so that QoS can be applied in transit (QoS tunnel pre-classification).

## Creating the Standard Priority Queue for an Interface

If you enable standard priority queueing for traffic on a physical interface, then you need to also create the priority queue on each interface. Each physical interface uses two queues: one for priority traffic, and the other for all other traffic. For the other traffic, you can optionally configure policing.



### Note

The standard priority queue is not required for hierarchical priority queueing with traffic shaping; see the [“Priority Queueing Overview”](#) section on page 25-3 for more information.

To create the priority queue, perform the following steps:

- Step 1** Go to Configuration > Device Management > Advanced > Priority Queue, and click **Add**.  
The Add Priority Queue dialog box displays.
- Step 2** From the Interface drop-down list, choose the physical interface name on which you want to enable the priority queue, or for the ASA 5505, the VLAN interface name.
- Step 3** To change the size of the priority queues, in the Queue Limit field, enter the number of average, 256-byte packets that the specified interface can transmit in a 500-ms interval.  
A packet that stays more than 500 ms in a network node might trigger a timeout in the end-to-end application. Such a packet can be discarded in each network node.  
Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped (called *tail drop*). To avoid having the queue fill up, you can use this option to increase the queue buffer size.  
The upper limit of the range of values for this option is determined dynamically at run time. The key determinants are the memory needed to support the queues and the memory available on the device.  
The Queue Limit that you specify affects both the higher priority low-latency queue and the best effort queue.
- Step 4** To specify the depth of the priority queues, in the Transmission Ring Limit field, enter the number of maximum 1550-byte packets that the specified interface can transmit in a 10-ms interval.

This setting guarantees that the hardware-based transmit ring imposes no more than 10-ms of extra latency for a high-priority packet.

This option sets the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears.

The upper limit of the range of values is determined dynamically at run time. The key determinants are the memory needed to support the queues and the memory available on the device.

The Transmission Ring Limit that you specify affects both the higher priority low-latency queue and the best-effort queue.

## Creating a Policy for Standard Priority Queueing and/or Policing

You can configure standard priority queueing and policing rules for the same interface. See the [“How QoS Features Interact” section on page 25-4](#) for information about valid QoS configurations.

To configure a QoS service policy, perform the following steps:

- 
- Step 1** To configure priority queueing, configure a service policy rule in the Configuration > Firewall > Service Policy Rules pane according to [Chapter 22, “Configuring Service Policy Rules.”](#)
- You can configure QoS as part of a new service policy rule, or you can edit an existing service policy.
- For priority traffic, identify only latency-sensitive traffic. You can match traffic based on many characteristics, including access lists, tunnel groups, DSCP, precedence, and more. You cannot use the **class-default** class map for priority traffic. You cannot configure priority queueing for the global policy if you also enable traffic shaping on any interfaces.
- Step 2** In the Rule Actions dialog box, click the **QoS** tab.
- Step 3** Click **Enable priority for this flow**.
- If this service policy rule is for an individual interface, ASDM automatically creates the priority queue for the interface (Configuration > Properties > Priority Queue; for more information, see the [“Creating the Standard Priority Queue for an Interface” section on page 25-5](#)). If this rule is for the global policy, then you need to manually add the priority queue to one or more interfaces *before* you configure the service policy rule.
- Step 4** Click **Finish**. The service policy rule is added to the rule table.
- Step 5** To configure policing, configure a service policy rule for the same interface in the Configuration > Firewall > Service Policy Rules pane according to [Chapter 22, “Configuring Service Policy Rules.”](#)
- For policing traffic, you can choose to police all traffic that you are not prioritizing, or you can limit the traffic to certain types.
- Step 6** In the Rule Actions dialog box, click the **QoS** tab.
- Step 7** Click **Enable policing**, then check the **Input policing** or **Output policing** (or both) check boxes to enable the specified type of traffic policing. For each type of traffic policing, configure the following fields:
- **Committed Rate**—The rate limit for this traffic flow; this is a value in the range 8000-20000000000, specifying the maximum speed (bits per second) allowed.

- **Conform Action**—The action to take when the rate is less than the conform-burst value. Values are transmit or drop.
- **Exceed Action**—Take this action when the rate is between the conform-rate value and the conform-burst value. Values are transmit or drop.
- **Burst Rate**—A value in the range 1000-512000000, specifying the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value.

**Step 8** Click **Finish**. The service policy rule is added to the rule table.

**Step 9** Click **Apply** to send the configuration to the device.

## Creating a Policy for Traffic Shaping and Hierarchical Priority Queueing

You can configure traffic shaping for all traffic on an interface, and optionally hierarchical priority queueing for a subset of latency-sensitive traffic. See the [“How QoS Features Interact”](#) section on page 25-4 for information about valid QoS configurations.



### Note

One side-effect of priority queueing 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 are false alarms in the case of priority queueing. You can configure the IPSec anti-replay window size to avoid possible false alarms. See the Configuration > VPN > IPSec > IPSec Rules > Enable Anti-replay window size option in the [“Crypto Maps”](#) section on page 34-9.

To configure a QoS service policy, perform the following steps:

**Step 1** Configure a service policy on the Configuration > Firewall > Service Policy Rules pane according to [Chapter 22, “Configuring Service Policy Rules.”](#)

You can configure QoS as part of a new service policy rule, or you can edit an existing service policy.

For traffic shaping, all traffic on an interface must be shaped. You can only use the **class-default** class map, which is automatically created by the security appliance, and which matches all traffic.

You cannot configure a separate traffic shaping rule on the same interface for which you configure a priority queueing rule (see the [“Creating a Policy for Standard Priority Queueing and/or Policing”](#) section on page 25-6); you can, however, configure priority queueing for a subset of shaped traffic under the traffic shaping rule. You also cannot configure traffic shaping for the global policy if you also enable priority queueing on any interfaces.

**Step 2** In the Rule Actions dialog box, click the **QoS** tab.

**Step 3** Click **Enable traffic shaping**, and configure the following fields:

- **Average Rate**—Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000.
- **Burst Size**—Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the Burst Size, the default value is equivalent to 4-milliseconds of traffic at the specified Average Rate. For example, if the average rate is 1000000 bits per second, 4 ms worth =  $1000000 * 4/1000 = 4000$ .

**Step 4** (Optional) To configure priority queueing for a subset of shaped traffic:

- a. Click **Enforce priority to selected shape traffic**.
- b. Click **Configure** to identify the traffic that you want to prioritize.  
You are prompted to identify the traffic for which you want to apply priority queueing.
- c. After you identify the traffic (see the [“Adding a Service Policy Rule for Through Traffic”](#) section on page 22-6), click **Next**.
- d. Click **Enable priority for this flow**.
- e. Click **Finish**.

You return to the QoS tab.



---

**Note** For this type of priority queueing, you do *not* need to create a priority queue on an interface (**Configuration > Properties > Priority Queue**).

---

**Step 5** Click **Finish**. The service policy rule is added to the rule table.

**Step 6** Click **Apply** to send the configuration to the device.

---



## CHAPTER 26

# Configuring Filter Rules

---

This chapter includes the following sections:

- [URL Filtering, page 26-1](#)
- [Filter Rules, page 26-5](#)

## URL Filtering

You can apply filtering to connection requests originating from a more secure network to a less secure network. Although you can use ACLs to prevent outbound access to specific content servers, managing usage this way is difficult because of the size and dynamic nature of the Internet. You can simplify configuration and improve security appliance performance by using a separate server running one of the following Internet filtering products:

- Websense Enterprise for filtering HTTP, HTTPS, and FTP.
- Secure Computing SmartFilter for filtering HTTP only. (Although some versions of Sentian support HTTPS, the security appliance only supports filtering HTTP with Sentian.)

Although security appliance performance is less affected when using an external server, users may notice longer access times to websites or FTP servers when the filtering server is remote from the security appliance.

When filtering is enabled and a request for content is directed through the security appliance, the request is sent to the content server and to the filtering server at the same time. If the filtering server allows the connection, the security appliance forwards the response from the content server to the originating client. If the filtering server denies the connection, the security appliance drops the response and sends a message or return code indicating that the connection was not successful.

If user authentication is enabled on the security appliance, then the security appliance also sends the user name to the filtering server. The filtering server can use user-specific filtering settings or provide enhanced reporting regarding usage.

This section includes the following topics:

- [Configuring URL Filtering, page 26-2](#)
- [URL Filtering Servers, page 26-2](#)
- [Advanced URL Filtering, page 26-4](#)

## Configuring URL Filtering

To enable filtering with an external filtering server, perform the following steps.

- 
- |               |                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Go to <b>Configuration &gt; Firewall &gt; URL Filter Servers</b> to specify an external filtering server. See <a href="#">URL Filtering Servers, page 26-2</a> .                                                                                                                                     |
| <b>Step 2</b> | (Optional) Buffer responses from the content server. See <a href="#">Advanced URL Filtering, page 26-4</a> .                                                                                                                                                                                         |
| <b>Step 3</b> | (Optional) Cache content server addresses to improve performance. See <a href="#">Advanced URL Filtering, page 26-4</a> .                                                                                                                                                                            |
| <b>Step 4</b> | Go to <b>Configuration &gt; Firewall &gt; Filter Rules</b> to configure filter rules. See <a href="#">Filter Rules, page 26-5</a> .                                                                                                                                                                  |
| <b>Step 5</b> | Configure the external filtering server. For more information refer to the following websites: <ul style="list-style-type: none"><li>• <a href="http://www.websense.com">http://www.websense.com</a></li><li>• <a href="http://www.securecomputing.com">http://www.securecomputing.com</a></li></ul> |
- 

## URL Filtering Servers

The URL Filtering Servers pane lets you specify the external filter server to use. You can identify up to four of the same type of filtering servers per context. In single mode a maximum of 16 of the same type of filtering servers are allowed. The security appliance uses the servers in order until a server responds. You can only configure a single type of server (Websense or Secure Computing SmartFilter) in your configuration.

**Note**

You must add the filtering server before you can configure filtering for HTTP, HTTPS, or FTP filtering rules.

**Fields**

The URL Filtering Server Type area includes the following fields:

- Websense—Enables the Websense URL filtering servers.
- Secure Computing SmartFilter—Enables the Secure Computing SmartFilter URL filtering server.
- Secure Computing SmartFilter Port—Specifies the Secure Computing SmartFilter port. The default is 4005.

The URL Filtering Servers area includes the following fields:

- Interface—Displays the interface connected to the filtering server.
- IP Address—Displays the IP address of the filtering server.
- Timeout—Displays the number of seconds after which the request to the filtering server times out.
- Protocol—Displays the protocol used to communicate with the filtering server.
- TCP Connections—Displays the maximum number of TCP connections allowed for communicating with the URL filtering server.
- Add—Adds a new filtering server, depending on whether you have selected Websense or Secure Computing SmartFilter. See the following topics for more information:



- [Add/Edit Parameters for Websense URL Filtering, page 26-3](#)
- [Add/Edit Parameters for Secure Computing SmartFilter URL Filtering, page 26-4](#)
- Insert Before—Adds a new filtering server in a higher priority position than the currently selected server.
- Insert After—Adds a new filtering server in a lower priority position than the currently selected server.
- Edit—Lets you modify parameters for the selected filtering server.
- Delete—Deletes the selected filtering server.

You can perform the following actions on this pane:

- Advanced—Displays advanced filtering parameters, including buffering caching, and long URL support.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

#### For More Information

[Advanced URL Filtering, page 26-4](#)

[Filter Rules, page 26-5](#)

## Add/Edit Parameters for Websense URL Filtering

- Interface—Specifies the interface on which the URL filtering server is connected.
- IP Address—Specifies the IP address of the URL filtering server.
- Timeout—Specifies the number of seconds after which the request to the filtering server times out.
- Protocol area
  - TCP 1—Uses TCP Version 1 for communicating with the Websense URL filtering server.
  - TCP 4—Uses TCP Version 4 for communicating with the Websense URL filtering server.
  - UDP 4—Uses UDP Version 4 for communicating with the Websense URL filtering server.
- TCP Connections—Specifies the maximum number of TCP connections allowed for communicating with the URL filtering server.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Parameters for Secure Computing SmartFilter URL Filtering

- Interface—Specifies the interface on which the URL filtering server is connected.
- IP Address—Specifies the IP address of the URL filtering server.
- Timeout—Specifies the number of seconds after which the request to the filtering server times out.
- Protocol area
  - TCP—Uses TCP for communicating with the Secure Computing SmartFilter URL filtering server.
  - UDP—Uses UDP for communicating with the Secure Computing SmartFilter URL filtering server.

TCP Connections—Specifies the maximum number of TCP connections allowed for communicating with the URL filtering server.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Advanced URL Filtering

### Fields

#### URL Cache Size area

After a user accesses a site, the filtering server can allow the security appliance to cache the server address for a certain amount of time, as long as every site hosted at the address is in a category that is permitted at all times. Then, when the user accesses the server again, or if another user accesses the server, the security appliance does not need to consult the filtering server again.



**Note** Requests for cached IP addresses are not passed to the filtering server and are not logged. As a result, this activity does not appear in any reports.

- Enable caching based on—Enables caching based on the specified criteria.
  - Destination Address—Caches entries based on the URL destination address. Choose this mode if all users share the same URL filtering policy on the Websense server.

- Source/Destination Address—Caches entries based on both the source address initiating the URL request as well as the URL destination address. Choose this mode if users do not share the same URL filtering policy on the server.
- Cache size—Specifies the size of the cache.

#### URL Buffer Size area

When a user issues a request to connect to a content server, the security appliance sends the request to the content server and to the filtering server at the same time. If the filtering server does not respond before the content server, the server response is dropped. This delays the web server response from the point of view of the web client because the client must reissue the request.

By enabling the HTTP response buffer, replies from web content servers are buffered and the responses are forwarded to the requesting client if the filtering server allows the connection. This prevents the delay that might otherwise occur.

- Enable buffering—Enables request buffering.
  - Number of 1550-byte buffers—Specifies the number of 1550-byte buffers. Valid values are from 1 to 128.

- Long URL Support area

By default, the security appliance considers an HTTP URL to be a long URL if it is greater than 1159 characters. For Websense servers, you can increase the maximum length allowed.

- Use Long URL—Enables long URLs for Websense filtering servers.
- Maximum Long URL Size—Specifies the maximum URL length allowed, up to a maximum of 4 KB.
- Memory Allocated for Long URL—Specifies the memory allocated for long URLs.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Filter Rules

The Filter Rules pane displays configured filter rules and provides options for adding new filter rules or modifying existing rules. A filter rule specifies the type of filtering to apply and the kind of traffic to which it should be applied.



#### Note

Before you can add an HTTP, HTTPS, or FTP filter rule, you must enable a URL filtering server. To enable a URL filtering server, use the Configuration > Firewall > URL Filtering Servers pane. For more information, see [URL Filtering, page 26-1](#).

### Benefits

The Filter Rules pane provides information about the filter rules that are currently configured on the security appliance. It also provides buttons that you can use to add or modify the filter rules and to increase or decrease the amount of detail shown in the pane.

Filtering allows greater control over any traffic that your security policy allows to pass through the security appliance. Instead of blocking access altogether, you can remove specific undesirable objects from HTTP traffic, such as ActiveX objects or Java applets, that may pose a security threat in certain situations. You can also use URL filtering to direct specific traffic to an external filtering server, such as Secure Computing SmartFilter or Websense. These servers can block traffic to specific sites or types of sites, as specified by your security policy.

Because URL filtering is CPU-intensive, using an external filtering server ensures that the throughput of other traffic is not affected. However, depending on the speed of your network and the capacity of your URL filtering server, the time required for the initial connection may be noticeably slower for filtered traffic.

### Fields

- No—Numeric identifier of the rule. Rules are applied in numeric order.
- Source—Source host or network to which the filtering action applies.
- Destination—Destination host or network to which the filtering action applies.
- Service—Identifies the protocol or service to which the filtering action applies.
- Action—Type of filtering action to apply.
- Options—Indicates the options that have been enabled for the specific action.
- Add—Displays the types of filter rules you can add. Clicking the rule type opens the Add Filter Rule dialog box for the specified filter rule type.
  - Add Filter ActiveX Rule
  - Add Filter Java Rule
  - Add Filter HTTP Rule
  - Add Filter HTTPS Rule
  - Add Filter FTP Rule
- Edit—Displays the Edit Filter Rule dialog box for editing the selected filtering rule.
- Delete—Deletes the selected filtering rule.
- Cut—Lets you to cut a filter rule and place it elsewhere.
- Copy—Lets you copy a filter rule.
- Paste—Lets you paste a filter rule elsewhere.
- Find—Lets you search for a filter rule. Clicking in this button brings up an extended toolbar. See [Filtering the Rule Table, page 26-9](#) for more information.
- Rule Diagram—Toggles the display of the Rule Diagram.
- Packet Trace—Launches the Packet Tracer utility.
- Use the Addresses tab to choose the source of the filter rule that you are choosing.
  - Type—Lets you choose a source from the drop-down list, selecting from All, IP Address Objects, IP Names, or Network Object groups.
  - Name—Lists the name(s) of the filter rule.

- Add—Lets you add a filter rule.
- Edit—Lets you edit a filter rule.
- Delete—Lets you delete a filter rule.
- Find—Lets you find a filter rule.
- Use the Services tab to choose a predefined filter rule.
  - Type—Lets you choose a source from the drop-down list, selecting from All, IP Address Objects, IP Names, or Network Object groups.
  - Name—Lists the name(s) of the filter rule.
  - Edit—Lets you edit a filter rule.
  - Delete—Lets you delete a filter rule.
  - Find—Lets you find a filter rule.
- Use the Time Ranges to choose a time range for the filter rule.
  - Add—Add—Lets you add a time range for the filter rule.
  - Edit—Lets you edit a time range for the filter rule.
  - Delete—Lets you delete a time range for a filter rule.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Filter Rule

Use the Add Filter Rule dialog box to specify the interface on which the rule applies, to identify the traffic to which it applies, or to configure a specific type of filtering action.



### Note

Before you can add an HTTP, HTTPS, or FTP filter rule, you must enable a URL filtering server. To enable a URL filtering server, use the Features > Configuration > Properties > URL Filtering window. For more information, see [URL Filtering](#).

### Fields

- Action—Provides the following drop-down list of different filtering actions to apply (the actions displayed depend upon the type of filter rule being created or edited):
  - Filter ActiveX
  - Do not filter ActiveX
  - Filter Java Applet
  - Do not filter Java Applet

- Filter HTTP (URL)
  - Do not filter HTTP (URL)
  - Filter HTTPS
  - Do not filter HTTPS
  - Filter FTP
  - Do not filter FTP
- Source—Enter the source of the traffic to which the filtering action applies. You can enter the source in one of the following ways:
  - any—Enter “any” (without quotation marks) to indicate any source address.
  - *name*—Enter a hostname.
  - *address/mask*—Enter an IP address and optional network mask. You can express the netmask in CIDR or dotted decimal notation. For example, you can enter 10.1.1.0/24 or 10.1.1.0/255.255.255.0.
  - ...—Opens the Browse Source dialog box. You can choose a host or address from the drop-down list.
- Destination—Identifies the destination of the traffic to which the filtering action applies. You can enter the destination in one of the following ways:
  - any—Enter “any” (without quotation marks) to indicate any destination address.
  - *name*—Enter a hostname.
  - *address/mask*—Enter an IP address and optional network mask. You can express the netmask in CIDR or dotted decimal notation. For example, you can enter 10.1.1.0/24 or 10.1.1.0/255.255.255.0.
  - ...—Opens the Browse Destination dialog box. You can choose a host or address from the drop-down list.
- Service —Identifies the service of the traffic to which the filtering action applies. You can enter the destination in one of the following ways:
  - *tcp/port*—The port number can be from 1 to 65535. Additionally, you can use the following modifiers with the TCP service:
    - !=—Not equal to. For example, !=tcp/443
    - <—Less than. For example, <tcp/2000.
    - >—Great than. For example, >tcp/2000.
    - —Range. For example, tcp/2000-3000.
  - *name*—Enter a well-known service name, such as http or ftp.
  - ...—Opens the Browse Service dialog box. You can choose a service from the drop-down list.
- HTTP Options—This area appears only for HTTP filter rules.
  - When URL exceeds maximum permitted size—Choose the action to take when the URL exceeds the specified size. You can choose to truncate the URL or block the traffic.
  - Allow outbound traffic if URL server is not available—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.

- Block users from connecting to an HTTP proxy server—Prevent HTTP requests made through a proxy server.
- **Truncate CGI parameters from URL sent to URL server**—The security appliance forwards only the CGI script location and the script name, without any parameters, to the filtering server.
- **HTTPS Options**—This area appears only when you choose the **Filter HTTPS** option from the drop-down list.
  - **Allow outbound traffic if URL server is not available**—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.
- **FTP Options**—This area appears only when you choose the **Filter FTP** option from the drop-down list.
  - **Allow outbound traffic if URL server is not available**—When enabled, if the URL filtering server is down or connectivity is interrupted to the security appliance, users will be able to connect without URL filtering being performed. If this is disabled, users will not be able to connect to Internet websites when the URL server is unavailable.
  - **Block interactive FTP sessions (block if absolute FTP path is not provided)**—When enabled, FTP requests are dropped if they use a relative pathname to the FTP directory.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Filtering the Rule Table

It can be difficult to find a specific rule if your rule table includes a lot of entries. You can apply a filter to the rule table to show only the rules specified by the filter. To filter the rule table, perform the following steps:

- 
- Step 1** Click **Find** on the toolbar. The Filter toolbar appears.
- Step 2** Choose the type of filter from the filter drop-down list:
- **Source**—Displays rules based on the specified source address or hostname.
  - **Destination**—Displays rules based on the specified destination address or hostname.
  - **Source or Destination**—Displays rules based on the specified source or destination address or hostname.
  - **Service**—Displays rules based on the specified service.
  - **Rule Type**—Displays rules based on the specified rule type.
  - **Query**—Displays rules based on a complex query comprise of source, destination, service, and rule type information.

- Step 3** For Source, Destination, Source or Destination, and Service filters, perform the following steps:
- Choose the match criteria from the drop-down list. Choose “is” (without the quotes) for exact string matches or choose “contains” for partial string matches.
  - Enter the string to match using one of the following methods:
    - Type the source, destination, or service name into the condition field.
    - Click ... to open a browse dialog from which you can choose existing services, IP addresses, or hostnames.
- Step 4** For Rule Type filter, choose the rule type from the list.
- Step 5** For Query filters, click **Define Query** and configure the complex query. For more information about configuring the complex query, see [Browse Source/Destination/Service, page 26-11](#).
- Step 6** To apply the filter to the rule table, click **Filter**.
- Step 7** To clear the filter from the rule table and display all rule entries, click **Clear**.
- 

## Define Query

The Define Query dialog box lets you define a rule table filter based on multiple criteria, such as source, destination, service, and rule type.

Once you create the query and click OK, the filter is immediately applied to the rule table. You can clear the filter by clicking **Clear**.

### Fields

- Source—IP address or hostname of the source. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Destination—IP address or hostname of the destination. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Source or Destination—IP address or hostname of the source or destination. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify a network mask using CIDR notation (address/bit-count). You can specify multiple addresses by separating them by commas (,).
- Service—The protocol/port or name of a service. Choose “is” for an exact match or choose “contains” for a partial match. Click ... to open up a selection dialog. You can specify multiple services by separating them by commas (,).
- Rule Type—Choose the rule type from the drop-down list.

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

[Filtering the Rule Table, page 26-9](#)

## Browse Source/Destination/Service

The Browse Source/Destination/Service dialog box lets you choose from existing IP address, name, or service objects.

**Fields**

- **Add**—Click to add a new IP address, name, or service object.
- **Edit**—Click to edit an existing IP address, name, or service object.
- **Filter/Clear**—Enter a string by which to filter the information shown in the dialog box. Click **Filter** to apply the filter to the information shown in the dialog box. Click **Clear** to remove the filter and display all objects.
- **Type**—Organizes the objects shown into types, such as IP Names, IP Address Objects, and so on.
- **Name**—The name of the object. For services, it is the service name. For IP Address objects, it is the IP address, for IP name objects, it is the hostname.
- **IP Address**—The IP address of the address object.
- **Netmask**—The network mask of the address object.
- **Protocol**—The network protocol used by the service (such as tcp, udp, or icmp).
- **Source Ports**—The source port used by the service.
- **Destination Ports**—The destination port used by the service.
- **ICMP Type**—The ICMP type (for example 9, which is a router advertisement).
- **Description (optional)**—Specifies a description for the object.
- **Source/Destination/Service button**—Click this to add the address or service object to the filter rule or query.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

[Filter Rules, page 26-5](#)

[URL Filtering, page 26-1](#)



## CHAPTER 27

# Configuring Advanced Firewall Protection

---

This chapter describes how to prevent network attacks by configuring protection features, and includes the following sections:

- [Configuring Threat Detection, page 27-1](#)
- [Configuring Connection Settings, page 27-6](#)
- [Configuring IP Audit, page 27-11](#)
- [Configuring the Fragment Size, page 27-17](#)
- [Configuring Anti-Spoofing, page 27-20](#)
- [Configuring TCP Options, page 27-20](#)
- [Configuring Global Timeouts, page 27-23](#)



**Note**

For Sun RPC server and encrypted traffic inspection settings, which you configure in the Configuration > Firewall > Advanced area (along with many of the topics in this chapter), see [Chapter 24, “Configuring Application Layer Protocol Inspection.”](#)

---

## Configuring Threat Detection

This section describes how to configure scanning threat detection and basic threat detection. Threat detection is available in single mode only.

This section includes the following topics:

- [Configuring Basic Threat Detection, page 27-1](#)
- [Configuring Scanning Threat Detection, page 27-3](#)
- [Configuring Threat Statistics, page 27-4](#)
- [Threat Detection Field Descriptions, page 27-5](#)

To view threat detection statistics, see the “[Firewall Dashboard Tab](#)” section on [page 1-17](#).

## Configuring Basic Threat Detection

Basic threat detection detects activity that might be related to an attack, such as a DoS attack. Basic threat detection is enabled by default.

This section includes the following topics:

- [Basic Threat Detection Overview, page 27-2](#)
- [Configuring Basic Threat Detection, page 27-2](#)

## Basic Threat Detection Overview

Using basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the following reasons:

- Denial by access lists
- Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length)
- Connection limits exceeded (both system-wide resource limits, and limits set in the configuration)
- DoS attack detected (such as an invalid SPI, Stateful Firewall check failure)
- Basic firewall checks failed (This option is a combined rate that includes all firewall-related packet drops in this bulleted list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.)
- Suspicious ICMP packets detected
- Packets failed application inspection
- Interface overload
- Scanning attack detected (This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the [“Configuring Scanning Threat Detection” section on page 27-3](#)) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.)
- Incomplete session detection such as TCP SYN attack detected or no data UDP session attack detected

When the security appliance detects a threat, it immediately sends a system log message (730100).

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

## Configuring Basic Threat Detection

To enable or disable basic threat detection, on the Configuration > Firewall > Threat Detection pane, click the **Enable Basic Threat Detection** check box.

By default, this option enables detection for certain types of security events, including packet drops and incomplete session detections. You can override the default settings for each type of event if desired.

If an event rate is exceeded, then the security appliance sends a system message. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst rate interval is 1/60th of the average rate interval or 10 seconds, whichever is higher. For each received event, the security appliance checks the average and burst rate limits; if both rates are exceeded, then the security appliance sends two separate system messages, with a maximum of one message for each rate type per burst period.

[Table 27-1](#) lists the default settings.

**Table 27-1 Basic Threat Detection Default Settings**

| Packet Drop Reason                                                                                                                                                             | Trigger Settings                           |                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|------------------------------------------------|
|                                                                                                                                                                                | Average Rate                               | Burst Rate                                     |
| <ul style="list-style-type: none"> <li>DoS attack detected</li> <li>Bad packet format</li> <li>Connection limits exceeded</li> <li>Suspicious ICMP packets detected</li> </ul> | 100 drops/sec over the last 600 seconds.   | 400 drops/sec over the last 10 second period.  |
|                                                                                                                                                                                | 80 drops/sec over the last 3600 seconds.   | 320 drops/sec over the last 60 second period.  |
| Scanning attack detected                                                                                                                                                       | 5 drops/sec over the last 600 seconds.     | 10 drops/sec over the last 10 second period.   |
|                                                                                                                                                                                | 4 drops/sec over the last 3600 seconds.    | 8 drops/sec over the last 60 second period.    |
| Incomplete session detected such as TCP SYN attack detected or no data UDP session attack detected (combined)                                                                  | 100 drops/sec over the last 600 seconds.   | 200 drops/sec over the last 10 second period.  |
|                                                                                                                                                                                | 80 drops/sec over the last 3600 seconds.   | 160 drops/sec over the last 60 second period.  |
| Denial by access lists                                                                                                                                                         | 400 drops/sec over the last 600 seconds.   | 800 drops/sec over the last 10 second period.  |
|                                                                                                                                                                                | 320 drops/sec over the last 3600 seconds.  | 640 drops/sec over the last 60 second period.  |
| <ul style="list-style-type: none"> <li>Basic firewall checks failed</li> <li>Packets failed application inspection</li> </ul>                                                  | 400 drops/sec over the last 600 seconds.   | 1600 drops/sec over the last 10 second period. |
|                                                                                                                                                                                | 320 drops/sec over the last 3600 seconds.  | 1280 drops/sec over the last 60 second period. |
| Interface overload                                                                                                                                                             | 2000 drops/sec over the last 600 seconds.  | 8000 drops/sec over the last 10 second period. |
|                                                                                                                                                                                | 1600 drops/sec over the last 3600 seconds. | 6400 drops/sec over the last 60 second period. |

## Configuring Scanning Threat Detection

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the security appliance scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

You can configure the security appliance to send system log messages about an attacker or you can automatically shun the host.



**Caution**

The scanning threat detection feature can affect the security appliance performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

To configure scanning threat detection, perform the following steps:

**Step 1**

To enable scanning threat detection, on the Configuration > Firewall > Threat Detection pane, click the **Enable Scanning Threat Detection** check box.

By default, the system log message 730101 is generated when a host is identified as an attacker.

The security appliance identifies a host as an attacker or as a target if the scanning threat rate is exceeded. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst event rate is 1/60th of the average rate interval or 10 seconds, whichever is higher. For each event detected that is considered to be part of a scanning attack, the security appliance checks the average and burst rate limits. If either rate is exceeded for traffic sent from a host, then that host is considered to be an attacker. If either rate is exceeded for traffic received by a host, then that host is considered to be a target.

Table 27-2 lists the default rate limits for scanning threat detection.

**Table 27-2 Default Rate Limits for Scanning Threat Detection**

| Average Rate                            | Burst Rate                                   |
|-----------------------------------------|----------------------------------------------|
| 5 drops/sec over the last 600 seconds.  | 10 drops/sec over the last 10 second period. |
| 5 drops/sec over the last 3600 seconds. | 10 drops/sec over the last 60 second period. |

**Step 2**

(Optional) To automatically terminate a host connection when the security appliance identifies the host as an attacker, check the **Shun Hosts detected by scanning threat** check box.

**Step 3**

(Optional) To except host IP addresses from being shunned, enter an address in the **Networks excluded from shun** field.

You can enter multiple addresses or subnets separated by commas. To choose a network from the list of IP address objects, click the ... button.

## Configuring Threat Statistics

You can configure the security appliance to collect extensive statistics. Threat detection statistics show both allowed and dropped traffic rates. By default, statistics for access lists are enabled.

To view threat detection statistics, see the “[Firewall Dashboard Tab](#)” section on page 1-17.



**Caution**

Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. Enabling statistics for hosts affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Enabling statistics for ports, however, has modest impact.

- To enable *all* statistics, on the Configuration > Firewall > Threat Detection pane, click the **Enable All Statistics** radio button.

- To disable *all* statistics, on the Configuration > Firewall > Threat Detection pane, click the **Disable All Statistics** radio button.
- To enable only certain statistics, on the Configuration > Firewall > Threat Detection pane, click the **Enable Only Following Statistics** radio button, and then check one or more of the following check boxes:
  - **Hosts**—Enables host statistics. The host statistics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
  - **Access Rules** (enabled by default)—Enables statistics for access rules.
  - **Port**—Enables statistics for TCP and UDP ports.
  - **Protocol**—Enables statistics for non-TCP/UDP IP protocols.

## Threat Detection Field Descriptions

The Threat Detection pane lets you configure basic and scanning threat detection.

### Fields

- **Basic Threat Detection**—Basic threat detection detects activity that might be related to an attack, such as a DoS attack. Basic threat detection is enabled by default.
  - **Enable Basic Threat Detection**—Enables basic threat detection. See the [“Configuring Basic Threat Detection” section on page 27-1](#) for more information.
- **Scanning Threat Detection**—The scanning threat detection feature determines when a host is performing a scan.
  - **Enable Scanning Threat Detection**—Enables scanning threat detection. See the [“Configuring Scanning Threat Detection” section on page 27-3](#) for more information.
  - **Shun Hosts detected by scanning threat**—Automatically terminates a host connection when the security appliance identifies the host as an attacker.
 

Networks excluded from shun—Excepts host IP addresses from being shunned. You can enter multiple addresses or subnets separated by commas. To choose a network from the list of IP address objects, click the ... button.
- **Scanning Threat Statistics**—Enables the security appliance to collect extensive statistics. Threat detection statistics show both allowed and dropped traffic rates. By default, statistics for access lists are enabled. To view threat detection statistics, see the [“Firewall Dashboard Tab” section on page 1-17](#).



### Caution

Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. Enabling statistics for hosts affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Enabling statistics for ports, however, has modest impact.

- **Disable All Statistics**—Disables all statistics.
- **Enable All Statistics**—Enables all statistics.
- **Enable only following statistics**—Enables specific statistics.

**Hosts**—Enables host statistics. The host statistics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.

**Access Rules**— (Enabled by default) Enables statistics for access rules.

**Port**—Enables statistics for TCP and UDP ports.

**Protocol**—Enables statistics for non-TCP/UDP IP protocols.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Configuring Connection Settings

This section describes how to set maximum TCP and UDP connections, maximum embryonic connections, maximum per-client connections, connection timeouts, dead connection detection, and how to disable TCP sequence randomization. This section also describes how to configure TCP normalization. The TCP normalization feature identifies abnormal packets that the security appliance can act on when they are detected; for example, the security appliance can allow, drop, or clear the packets. TCP normalization helps protect the security appliance from attacks.

This section includes the following topics:

- [Connection Limit Overview, page 27-6](#)
- [TCP Normalization Overview, page 27-8](#)
- [Enabling Connection Limits and TCP Normalization, page 27-8](#)



### Note

You can also configure maximum connections, maximum embryonic connections, and TCP sequence randomization in the NAT configuration. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

## Connection Limit Overview

This section describes why you might want to limit connections, and includes the following topics:

- [TCP Intercept Overview, page 27-7](#)
- [Disabling TCP Intercept for Management Packets for Clientless SSL VPN Compatibility, page 27-7](#)
- [Dead Connection Detection Overview, page 27-7](#)
- [TCP Sequence Randomization Overview, page 27-7](#)



## TCP Intercept Overview

Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the security appliance acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the security appliance receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

## Disabling TCP Intercept for Management Packets for Clientless SSL VPN Compatibility

By default, TCP management connections have TCP Intercept always enabled. When TCP Intercept is enabled, it intercepts the 3-way TCP connection establishment handshake packets and thus deprives the security appliance from processing the packets for Clientless (browser-based) SSL VPN. Clientless SSL VPN requires the ability to process the 3-way handshake packets to provide selective ACK and other TCP options for Clientless SSL VPN connections. To disable TCP Intercept for management traffic, you can set the embryonic connection limit; only after the embryonic connection limit is reached is TCP Intercept enabled.

## Dead Connection Detection Overview

Dead connection detection detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist.

When you enable DCD, idle timeout behavior changes. With idle timeout, DCD probes are sent to each of the two end-hosts to determine the validity of the connection. If an end-host fails to respond after probes are sent at the configured intervals, the connection is freed, and reset values, if configured, are sent to each of the end-hosts. If both end-hosts response that the connection is valid, the activity timeout is updated to the current time and the idle timeout is rescheduled accordingly.

## TCP Sequence Randomization Overview

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predefining the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.

## TCP Normalization Overview

The TCP normalizer includes non-configurable actions and configurable actions. Typically, non-configurable actions that drop or clear connections apply to packets that are always bad. Configurable actions (as detailed in [“Enabling Connection Limits and TCP Normalization”](#) section on page 27-8) might need to be customized depending on your network needs.

See the following guidelines for TCP normalization:

- The normalizer does not protect from SYN floods. The security appliance includes SYN flood protection in other ways.
- The normalizer always sees the SYN packet as the first packet in a flow unless the security appliance is in loose mode due to failover.

## Enabling Connection Limits and TCP Normalization

To configure connection limits and TCP normalization, perform the following steps:

- 
- Step 1** Configure a service policy on the Configuration > Firewall > Service Policy Rules pane according to [Chapter 22, “Configuring Service Policy Rules.”](#)
- You can configure connection limits as part of a new service policy rule, or you can edit an existing service policy.
- Step 2** On the Rule Actions dialog box, click the **Connection Settings** tab.
- Step 3** To set maximum connections, configure the following values in the Maximum Connections area:
- **TCP & UDP Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for all clients in the traffic class, up to 65,536. The default is 0 for both protocols, which means the maximum possible connections are allowed.
  - **Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped. Thus, connection attempts from unreachable hosts will never reach the server.
  - **Per Client Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for each client. When a new connection is attempted by a client that already has opened the maximum per-client number of connections, the security appliance rejects the connection and drops the packet.
  - **Per Client Embryonic Connections**—Specifies the maximum number of simultaneous TCP embryonic connections for each client. When a new TCP connection is requested by a client that already has the maximum per-client number of embryonic connections open through the security appliance, the security appliance proxies the request to the TCP Intercept feature, which prevents the connection.
- Step 4** To configure TCP timeouts, configure the following values in the TCP Timeout area:
- **Connection Timeout**—Specifies the idle time until a connection slot is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is 1 hour.

- Send reset to TCP endpoints before timeout—Specifies that the security appliance should send a TCP reset message to the endpoints of the connection before freeing the connection slot.
- Embryonic Connection Timeout—Specifies the idle time until an embryonic connection slot is freed. Enter 0:0:0 to disable timeout for the connection. The default is 30 seconds.
- Half Closed Connection Timeout—Specifies the idle time until a half closed connection slot is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is 10 minutes.

**Step 5** To disable randomized sequence numbers, uncheck **Randomize Sequence Number**.

TCP initial sequence number randomization can be disabled if another in-line firewall is also randomizing the initial sequence numbers, because there is no need for both firewalls to be performing this action. However, leaving ISN randomization enabled on both firewalls does not affect the traffic.

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in the outbound direction. If the connection is between two interfaces with the same security level, then the ISN will be randomized in the SYN in both directions.

Randomizing the ISN of the protected host prevents an attacker from predefining the next ISN for a new connection and potentially hijacking the new session.

**Step 6** To configure TCP normalization, check **Use TCP Map**.

Choose an existing TCP map from the drop-down list (if available), or add a new one by clicking **New**. The Add TCP Map dialog box appears.

- a. In the TCP Map Name field, enter a name.
- b. In the Queue Limit field, enter the maximum number of out-of-order packets, between 0 and 250 packets.

The Queue Limit sets the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection. The default is 0, which means this setting is disabled and the default system queue limit is used depending on the type of traffic:

- Connections for application inspection, IPS, and TCP check-retransmission have a queue limit of 3 packets. If the security appliance receives a TCP packet with a different window size, then the queue limit is dynamically changed to match the advertised setting.
- For other TCP connections, out-of-order packets are passed through untouched.

If you set the Queue Limit command to be 1 or above, then the number of out-of-order packets allowed for all TCP traffic matches this setting. For application inspection, IPS, and TCP check-retransmission traffic, any advertised settings are ignored. For other TCP traffic, out-of-order packets are now buffered and put in order instead of passed through untouched.

- c. In the Timeout field, set the maximum amount of time that out-of-order packets can remain in the buffer, between 1 and 20 seconds.

If they are not put in order and passed on within the timeout period, then they are dropped. The default is 4 seconds. You cannot change the timeout for any traffic if the Queue Limit is set to 0; you need to set the limit to be 1 or above for the Timeout to take effect.

- d. In the Reserved Bits area, click **Clear and allow**, **Allow only**, or **Drop**.

Allow only allows packets with the reserved bits in the TCP header.

Clear and allow clears the reserved bits in the TCP header and allows the packet.

Drop drops the packet with the reserved bits in the TCP header.

- e. Check any of the following options:

- Clear urgent flag—Clears the URG flag through the security appliance. The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks.
- Drop connection on window variation—Drops a connection that has changed its window size unexpectedly. The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged. When this condition is detected, the connection can be dropped.
- Drop packets that exceed maximum segment size—Drops packets that exceed MSS set by peer.
- Check if transmitted data is the same as original—Enables the retransmit data checks.
- Drop packets which have past-window sequence—Drops packets that have past-window sequence numbers, namely the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window. If you do not check this option, then the Queue Limit must be set to 0 (disabled).
- Drop SYN Packets with data—Drops SYN packets with data.
- Drop SYNACK Packets with data—Drops TCP SYNACK packets that contain data.
- Drop packets with invalid ACK—Drops packets with an invalid ACK. You might see invalid ACKs in the following instances:
  - In the TCP connection SYN-ACK-received status, if the ACK number of a received TCP packet is not exactly same as the sequence number of the next TCP packet sending out, it is an invalid ACK.
  - Whenever the ACK number of a received TCP packet is greater than the sequence number of the next TCP packet sending out, it is an invalid ACK.




---

**Note** TCP packets with an invalid ACK are automatically allowed for WAAS connections.

---

- Enable TTL Evasion Protection—Enables the TTL evasion protection offered by the security appliance. Do not enable this option if you want to prevent attacks that attempt to evade security policy.  
 For example, an attacker can send a packet that passes policy with a very short TTL. When the TTL goes to zero, a router between the security appliance and the endpoint drops the packet. It is at this point that the attacker can send a malicious packet with a long TTL that appears to the security appliance to be a retransmission and is passed. To the endpoint host, however, it is the first packet that has been received by the attacker. In this case, an attacker is able to succeed without security preventing the attack.
  - Verify TCP Checksum—Enables checksum verification.
- f. To set TCP options, check any of the following options:
- Clear Selective Ack—Lists whether the selective-ack TCP option is allowed or cleared.
  - Clear TCP Timestamp—Lists whether the TCP timestamp option is allowed or cleared.
  - Clear Window Scale—Lists whether the window scale timestamp option is allowed or cleared.
  - Range—Lists the valid TCP options ranges, which should fall within 6-7 and 9-255. The lower bound should be less than or equal to the upper bound.
- g. Click **OK**.

- Step 7** To set the time to live, check **Decrement time to live for a connection**.
- Step 8** Click **OK** or **Finish**.
- 

## Configuring IP Audit

The IP audit feature provides basic IPS functionality; for advanced IPS functionality on supported platforms, you can install an AIP SSM.

This feature lets you create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature. Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. You can configure the security appliance to drop the packet, generate an alarm, or reset the connection.

## IP Audit Policy

The IP Audit Policy pane lets you add audit policies and assign them to interfaces. You can assign an attack policy and an informational policy to each interface. The attack policy determines the action to take with packets that match an attack signature; the packet might be part of an attack on your network, such as a DoS attack. The informational policy determines the action to take with packets that match an informational signature; the packet is not currently attacking your network, but could be part of an information-gathering activity, such as a port sweep. For a complete list of signatures, see the [IP Audit Signature List](#).

### Fields

- **Name**—Shows the names of the defined IP audit policies. Although the default actions for a named policy are listed in this table (“--Default Action--”), they are not named policies that you can assign to an interface. Default actions are used by named policies if you do not set an action for the policy. You can modify the default actions by selecting them and clicking the Edit button.
- **Type**—Shows the policy type, either Attack or Info.
- **Action**—Shows the actions taken against packets that match the policy, Alarm, Drop, and/or Reset. Multiple actions can be listed.
- **Add**—Adds a new IP audit policy.
- **Edit**—Edits an IP audit policy or the default actions.
- **Delete**—Deletes an IP audit policy. You cannot delete a default action.
- **Policy-to-Interface Mappings**—Assigns an attack and informational policy to each interface.
  - **Interface**—Shows the interface name.
  - **Attack Policy**—Lists the attack audit policy names available. Assign a policy to an interface by clicking the name in the list.
  - **Info Policy**—Lists the informational audit policy names available. Assign a policy to an interface by clicking the name in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit IP Audit Policy Configuration

The Add/Edit IP Audit Policy Configuration dialog box lets you add or edit a named IP audit policy that you can assign to interfaces, and lets you modify the default actions for each signature type.

### Fields

- Policy Name—Sets the IP audit policy name. You cannot edit the name after you add it.
- Policy Type—Sets the policy type. You cannot edit the policy type after you add it.
  - Attack—Sets the policy type as attack.
  - Information—Sets the policy type as informational.
- Action—Sets one or more actions to take when a packet matches a signature. If you do not choose an action, then the default policy is used.
  - Alarm—Generates a system message showing that a packet matched a signature. For a complete list of signatures, see [IP Audit Signature List](#).
  - Drop—Drops the packet.
  - Reset—Drops the packet and closes the connection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## IP Audit Signatures

The IP Audit Signatures pane lets you disable audit signatures. You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms.

For a complete list of signatures, see [IP Audit Signature List](#).

### Fields

- Enabled—Lists the enabled signatures.
- Disabled—Lists the disabled signatures.

- Disable—Moves the selected signature to the Disabled pane.
- Enable—Moves the selected signature to the Enabled pane.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## IP Audit Signature List

Table 27-3 lists supported signatures and system message numbers.

**Table 27-3** Signature IDs and System Message Numbers

| Signature ID | Message Number | Signature Title                | Signature Type | Description                                                                                                                                                                                                                           |
|--------------|----------------|--------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1000         | 400000         | IP options-Bad Option List     | Informational  | Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks. |
| 1001         | 400001         | IP options-Record Packet Route | Informational  | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).                                                                                                              |
| 1002         | 400002         | IP options-Timestamp           | Informational  | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).                                                                                                                        |
| 1003         | 400003         | IP options-Security            | Informational  | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).                                                                                                                 |
| 1004         | 400004         | IP options-Loose Source Route  | Informational  | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).                                                                                                               |
| 1005         | 400005         | IP options-SATNET ID           | Informational  | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).                                                                                                         |
| 1006         | 400006         | IP options-Strict Source Route | Informational  | Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).                                                                                                         |
| 1100         | 400007         | IP Fragment Attack             | Attack         | Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.                                                                                                          |

**Table 27-3** Signature IDs and System Message Numbers (continued)

| Signature ID | Message Number | Signature Title                     | Signature Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|----------------|-------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1102         | 400008         | IP Impossible Packet                | Attack         | Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.                                                                                                                                                                                                                                                                                                                                                                                                             |
| 1103         | 400009         | IP Overlapping Fragments (Teardrop) | Attack         | Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS. |
| 2000         | 400010         | ICMP Echo Reply                     | Informational  | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).                                                                                                                                                                                                                                                                                                                                                                                 |
| 2001         | 400011         | ICMP Host Unreachable               | Informational  | Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).                                                                                                                                                                                                                                                                                                                                                                          |
| 2002         | 400012         | ICMP Source Quench                  | Informational  | Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).                                                                                                                                                                                                                                                                                                                                                                             |
| 2003         | 400013         | ICMP Redirect                       | Informational  | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).                                                                                                                                                                                                                                                                                                                                                                                   |
| 2004         | 400014         | ICMP Echo Request                   | Informational  | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).                                                                                                                                                                                                                                                                                                                                                                               |
| 2005         | 400015         | ICMP Time Exceeded for a Datagram   | Informational  | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11 (Time Exceeded for a Datagram).                                                                                                                                                                                                                                                                                                                                                              |
| 2006         | 400016         | ICMP Parameter Problem on Datagram  | Informational  | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).                                                                                                                                                                                                                                                                                                                                                             |



**Table 27-3**      *Signature IDs and System Message Numbers (continued)*

| <b>Signature ID</b> | <b>Message Number</b> | <b>Signature Title</b>    | <b>Signature Type</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------|---------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2007                | 400017                | ICMP Timestamp Request    | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).                                                                                                                                                                                                                                           |
| 2008                | 400018                | ICMP Timestamp Reply      | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).                                                                                                                                                                                                                                             |
| 2009                | 400019                | ICMP Information Request  | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).                                                                                                                                                                                                                                         |
| 2010                | 400020                | ICMP Information Reply    | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).                                                                                                                                                                                                                                      |
| 2011                | 400021                | ICMP Address Mask Request | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).                                                                                                                                                                                                                                        |
| 2012                | 400022                | ICMP Address Mask Reply   | Informational         | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).                                                                                                                                                                                                                                          |
| 2150                | 400023                | Fragmented ICMP Traffic   | Attack                | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.                                                                                                                                                                                                     |
| 2151                | 400024                | Large ICMP Traffic        | Attack                | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the IP length > 1024.                                                                                                                                                                                                                                                                                      |
| 2154                | 400025                | Ping of Death Attack      | Attack                | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP), the Last Fragment bit is set, and $(IP\ offset * 8) + (IP\ data\ length) > 65535$ that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet. |
| 3040                | 400026                | TCP NULL flags            | Attack                | Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.                                                                                                                                                                                                                                                                                            |

Table 27-3 Signature IDs and System Message Numbers (continued)

| Signature ID | Message Number | Signature Title                           | Signature Type | Description                                                                                                                                             |
|--------------|----------------|-------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3041         | 400027         | TCP SYN+FIN flags                         | Attack         | Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.                                                    |
| 3042         | 400028         | TCP FIN only flags                        | Attack         | Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.                     |
| 3153         | 400029         | FTP Improper Address Specified            | Informational  | Triggers if a port command is issued with an address that is not the same as the requesting host.                                                       |
| 3154         | 400030         | FTP Improper Port Specified               | Informational  | Triggers if a port command is issued with a data port specified that is <1024 or >65535.                                                                |
| 4050         | 400031         | UDP Bomb attack                           | Attack         | Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt. |
| 4051         | 400032         | UDP Snork attack                          | Attack         | Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.                                        |
| 4052         | 400033         | UDP Chargen DoS attack                    | Attack         | This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.                                             |
| 6050         | 400034         | DNS HINFO Request                         | Informational  | Triggers on an attempt to access HINFO records from a DNS server.                                                                                       |
| 6051         | 400035         | DNS Zone Transfer                         | Informational  | Triggers on normal DNS zone transfers, in which the source port is 53.                                                                                  |
| 6052         | 400036         | DNS Zone Transfer from High Port          | Informational  | Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.                                                             |
| 6053         | 400037         | DNS Request for All Records               | Informational  | Triggers on a DNS request for all records.                                                                                                              |
| 6100         | 400038         | RPC Port Registration                     | Informational  | Triggers when attempts are made to register new RPC services on a target host.                                                                          |
| 6101         | 400039         | RPC Port Unregistration                   | Informational  | Triggers when attempts are made to unregister existing RPC services on a target host.                                                                   |
| 6102         | 400040         | RPC Dump                                  | Informational  | Triggers when an RPC dump request is issued to a target host.                                                                                           |
| 6103         | 400041         | Proxied RPC Request                       | Attack         | Triggers when a proxied RPC request is sent to the portmapper of a target host.                                                                         |
| 6150         | 400042         | ypserv (YP server daemon) Portmap Request | Informational  | Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.                                                               |

**Table 27-3**      *Signature IDs and System Message Numbers (continued)*

| Signature ID | Message Number | Signature Title                                 | Signature Type | Description                                                                                                                                                                                                                  |
|--------------|----------------|-------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6151         | 400043         | ybind (YP bind daemon) Portmap Request          | Informational  | Triggers when a request is made to the portmapper for the YP bind daemon (ybind) port.                                                                                                                                       |
| 6152         | 400044         | yppasswdd (YP password daemon) Portmap Request  | Informational  | Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.                                                                                                                               |
| 6153         | 400045         | ypupdated (YP update daemon) Portmap Request    | Informational  | Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.                                                                                                                                 |
| 6154         | 400046         | ypxfrd (YP transfer daemon) Portmap Request     | Informational  | Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.                                                                                                                                  |
| 6155         | 400047         | mountd (mount daemon) Portmap Request           | Informational  | Triggers when a request is made to the portmapper for the mount daemon (mountd) port.                                                                                                                                        |
| 6175         | 400048         | rexed (remote execution daemon) Portmap Request | Informational  | Triggers when a request is made to the portmapper for the remote execution daemon (rexed) port.                                                                                                                              |
| 6180         | 400049         | rexed (remote execution daemon) Attempt         | Informational  | Triggers when a call to the rexed program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources. |
| 6190         | 400050         | statd Buffer Overflow                           | Attack         | Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.                                                                                              |

## Configuring the Fragment Size

By default, the security appliance allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to let fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, if you do not have an application that fragments traffic, we recommend that you do not allow fragments through the security appliance. Fragmented packets are often used as DoS attacks.

### Fields

- Fragment table:
  - Interface—Lists the available interfaces of the security appliance.
  - Size—Sets the maximum number of packets that can be in the IP reassembly database waiting for reassembly. The default is 200.
  - Chain Length—Specifies the maximum number of packets into which a full IP packet can be fragmented. The default is 24 packets.

- **Timeout**—Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded. The default is 5 seconds.
- **Edit**—Opens the Edit Fragment dialog box.
- **Show Fragment**—Opens a panel and displays the current IP fragment database statistics for each interface of the security appliance.

### Changing Fragment Parameters

To modify the IP fragment database parameters of an interface, perform the following steps:

- 
- Step 1** Choose the interface to change in the Fragment table and click **Edit**. The Edit Fragment dialog box appears.
- Step 2** In the Edit Fragment dialog box, change the Size, Chain, and Timeout values as desired, and click **OK**. If you make a mistake, click **Restore Defaults**.
- Step 3** Click **Apply** in the Fragment panel.
- 

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Show Fragment

The Show Fragment panel displays the operational data of the IP fragment reassembly module.

### Fields

- **Size**—*Display only*. Displays the number of packets in the IP reassembly database waiting for reassembly. The default is 200.
- **Chain**—*Display only*. Displays the number of packets into which a full IP packet can be fragmented. The default is 24 packets.
- **Timeout**—*Display only*. Displays the number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds displayed, all fragments of the packet that were already received will be discarded. The default is 5 seconds.
- **Threshold**—*Display only*. Displays the IP packet threshold, or the limit after which no new chains can be created in the reassembly module.
- **Queue**—*Display only*. Displays the number of IP packets waiting in the queue for reassembly.
- **Assembled**—*Display only*. Displays the number of IP packets successfully reassembled.

- Fail—*Display only*. Displays the number of failed reassembly attempts.
- Overflow—*Display only*. Displays the number of IP packets in the overflow queue.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Edit Fragment

The Edit Fragment dialog box lets you configure the IP fragment database of the selected interface.

### Fields

- Interface—Displays the interface you selected in the Fragment panel. Changes made in the Edit Fragment dialog box are applied to the interface displayed.
- Size—Sets the maximum number of packets that can be in the IP reassembly database waiting for reassembly.
- Chain Length—Sets the maximum number of packets into which a full IP packet can be fragmented.
- Timeout—Sets the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.
- Restore Defaults—Restores the factory default settings:
  - Size is 200.
  - Chain is 24 packets.
  - Timeout is 5 seconds.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Configuring Anti-Spoofing

The Anti-Spoofing window lets you enable Unicast Reverse Path Forwarding on an interface. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

Normally, the security appliance only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the security appliance to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the security appliance can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the security appliance uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

### Fields

- Interface—Lists the interface names.
- Anti-Spoofing Enabled—Shows whether an interface has Unicast RPF enabled, Yes or No.
- Enable—Enables Unicast RPF for the selected interface.
- Disable—Disables Unicast RPF for the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | •        | —      |

## Configuring TCP Options

The TCP Options pane lets you set parameters for TCP connections.

**Fields**

- Inbound and Outbound Reset—Sets whether to reset denied TCP connections for inbound and outbound traffic.
  - Interface—Shows the interface name.
  - Inbound Reset—Shows the interface reset setting for inbound TCP traffic, Yes or No. Enabling this setting causes the security appliance to send TCP resets for all inbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets.
  - Outbound Reset—Shows the interface reset setting for outbound TCP traffic, Yes or No. Enabling this setting causes the security appliance to send TCP resets for all outbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets.
  - Edit—Sets the inbound and outbound reset settings for the interface.
- Other Options—Sets additional TCP options.
  - Send Reset Reply for Denied Outside TCP Packets—Enables resets for TCP packets that terminate at the least secure interface and are denied by the security appliance based on access lists or AAA settings. When this option is not enabled, the security appliance silently discards denied packets. If you enable Inbound Resets for the least secure interface (see [TCP Reset Settings](#)), then you do not also have to enable this setting; Inbound Resets handle to-the-security appliance traffic as well as through the security appliance traffic.
  - Force Maximum Segment Size for TCP—Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting the bytes to 0. Both the host and the server can set the maximum segment size when they first establish a connection. If either maximum exceeds the value you set here, then the security appliance overrides the maximum and inserts the value you set. For example, if you set a maximum size of 1200 bytes, when a host requests a maximum size of 1300 bytes, then the security appliance alters the packet to request 1200 bytes.
  - Force Minimum Segment Size for TCP—Overrides the maximum segment size to be no less than the number of bytes you set, between 48 and any maximum number. This feature is disabled by default (set to 0). Both the host and the server can set the maximum segment size when they first establish a connection. If either maximum is less than the value you set for the Force Minimum Segment Size for TCP Proxy field, then the security appliance overrides the maximum and inserts the “minimum” value you set (the minimum value is actually the smallest maximum allowed). For example, if you set a minimum size of 400 bytes, if a host requests a maximum value of 300 bytes, then the security appliance alters the packet to request 400 bytes.
  - Force TCP Connection to Linger in TIME\_WAIT State for at Least 15 Seconds—Forces each TCP connection to linger in a shortened TIME\_WAIT state of at least 15 seconds after the final normal TCP close-down sequence. You might want to use this feature if an end host application default TCP terminating sequence is a simultaneous close. The default behavior of the security appliance is to track the shutdown sequence and release the connection after two FINs and the ACK of the last FIN segment. This quick release heuristic enables the security appliance to sustain a high connection rate, based on the most common closing sequence, known as the normal close sequence. However, in a simultaneous close, both ends of the transaction initiate the closing sequence, as opposed to the normal close sequence where one end closes and the other end acknowledges prior to initiating its own closing sequence (see RFC 793). Thus, in a simultaneous close, the quick release forces one side of the connection to linger in the

CLOSING state. Having many sockets in the CLOSING state can degrade the performance of an end host. For example, some WinSock mainframe clients are known to exhibit this behavior and degrade the performance of the mainframe server. Using this feature creates a window for the simultaneous close down sequence to complete.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## TCP Reset Settings

This dialog box sets the inbound and outbound reset settings for an interface.

### Fields

- Send Reset Reply for Denied Inbound TCP Packets—Sends TCP resets for all inbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets.

You might want to explicitly send resets for inbound traffic if you need to reset identity request (IDENT) connections. When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance.

- Send Reset Reply for Denied Outbound TCP Packets—Sends TCP resets for all outbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets. This option is enabled by default. You might want to disable outbound resets to reduce the CPU load during traffic storms, for example.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |



# Configuring Global Timeouts

The Timeouts pane lets you set the timeout durations for use with the security appliance. All durations are displayed in the format hh:mm:ss. It sets the idle time for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP\_connection slots are freed approximately 60 seconds after a normal connection close sequence.

**Note**

It is recommended that you do not change these values unless advised to do so by Customer Support.

**Fields**

In all cases, except for Authentication absolute and Authentication inactivity, unchecking the check boxes means there is no timeout value. For those two cases, clearing the check box means to reauthenticate on every new connection.

- **Connection**—Modifies the idle time until a connection slot is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is 1 hour.
- **Half-closed**—Modifies the idle time until a TCP half-closed connection closes. The minimum is 5 minutes. The default is 10 minutes. Enter 0:0:0 to disable timeout for a half-closed connection.
- **UDP**—Modifies the idle time until a UDP protocol connection closes. This duration must be at least 1 minute. The default is 2 minutes. Enter 0:0:0 to disable timeout.
- **ICMP**—Modifies the idle time after which general ICMP states are closed.
- **H.323**—Modifies the idle time until an H.323 media connection closes. The default is 5 minutes. Enter 0:0:0 to disable timeout.
- **H.225**—Modifies the idle time until an H.225 signaling connection closes. The H.225 default timeout is 1 hour (01:00:00). Setting the value of 00:00:00 means never close this connection. To close this connection immediately after all calls are cleared, a value of 1 second (00:00:01) is recommended.
- **MGCP**—Modifies the timeout value for MGCP which represents the idle time after which MGCP media ports are closed. The MGCP default timeout is 5 minutes (00:05:00). Enter 0:0:0 to disable timeout.
- **MGCP PAT**—Modifies the idle time after which an MGCP PAT translation is removed. The default is 5 minutes (00:05:00). The minimum time is 30 seconds. Uncheck the check box to return to the default value.
- **SUNRPC**—Modifies the idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes. Enter 0:0:0 to disable timeout.
- **SIP**—Modifies the idle time until an SIP signalling port connection closes. This duration must be at least 5 minutes. The default is 30 minutes.
- **SIP Media**—Modifies the idle time until an SIP media port connection closes. This duration must be at least 1 minute. The default is 2 minutes.
- **SIP Provisional Media**—Modifies the timeout value for SIP provisional media connections, between 0:1:0 and 1193:0:0. The default is 2 minutes.
- **SIP Invite**—Modifies the idle time after which pinholes for PROVISIONAL responses and media xlates will be closed. The minimum value is 0:1:0, the maximum value is 0:30:0. The default value is 0:03:00.

- SIP Disconnect—Modifies the idle time after which SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message. The minimum value is 0:0:1, the maximum value is 0:10:0. The default value is 0:02:00.
- Authentication absolute—Modifies the duration until the authentication cache times out and you have to reauthenticate a new connection. This duration must be shorter than the Translation Slot value. The system waits until you start a new connection to prompt you again. Enter 0:0:0 to disable caching and reauthenticate on every new connection.



**Note** Do not set this value to 0:0:0 if passive FTP is used on the connections.



**Note** When Authentication Absolute = 0, HTTPS authentication may not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is permitted through, but subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even after successful authentication. To work around this, set the authentication absolute timeout to 1 second. This workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.

- Authentication inactivity—Modifies the idle time until the authentication cache times out and users have to reauthenticate a new connection. This duration must be shorter than the Translation Slot value.
- Translation Slot—Modifies the idle time until a translation slot is freed. This duration must be at least 1 minute. The default is 3 hours. Enter 0:0:0 to disable timeout.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |



# CHAPTER 28

## Configuring IPS

---

This chapter describes how to configure the adaptive security appliance to support an AIP SSM that is installed in the security appliance.



### Note

---

The Cisco PIX 500 series security appliances do not support SSMs.

---

This chapter includes the following sections:

- [AIP SSM Overview, page 28-1](#)
- [Accessing IDM from ASDM, page 28-5](#)
- [Configuring the AIP SSM Security Policy in IDM, page 28-5](#)
- [Assigning Virtual Sensors to Security Contexts, page 28-5](#)
- [Diverting Traffic to the AIP SSM, page 28-6](#)
- [Resetting the AIP SSM Password, page 28-8](#)

## AIP SSM Overview

You can install the AIP SSM into an ASA 5500 series adaptive security appliance. The AIP SSM runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. This section includes the following topics:

- [How the AIP SSM Works with the Adaptive Security Appliance, page 28-2](#)
- [Operating Modes, page 28-2](#)
- [Using Virtual Sensors, page 28-3](#)
- [AIP SSM Procedure Overview, page 28-4](#)

## How the AIP SSM Works with the Adaptive Security Appliance

The AIP SSM runs a separate application from the adaptive security appliance. It is, however, integrated into the adaptive security appliance traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you identify traffic for IPS inspection on the adaptive security appliance, traffic flows through the adaptive security appliance and the AIP SSM in the following way:

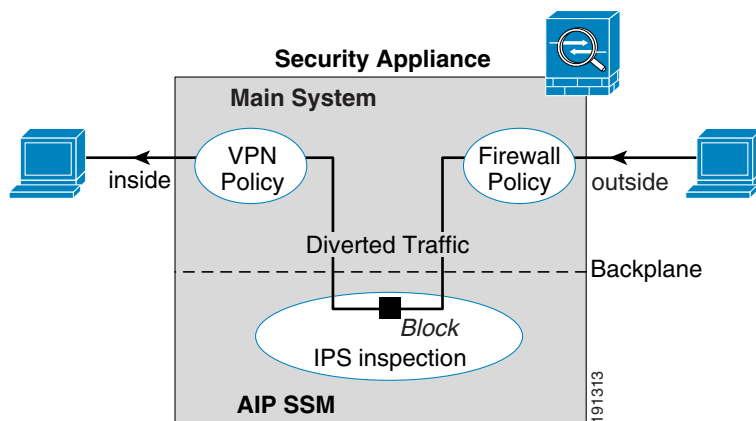
1. Traffic enters the adaptive security appliance.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane.

See the [“Operating Modes” section on page 28-2](#) for information about only sending a copy of the traffic to the AIP SSM.

4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the adaptive security appliance over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the adaptive security appliance.

[Figure 28-1](#) shows the traffic flow when running the AIP SSM in inline mode. In this example, the AIP SSM automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the security appliance.

**Figure 28-1 AIP SSM Traffic Flow in the Adaptive Security Appliance: Inline Mode**



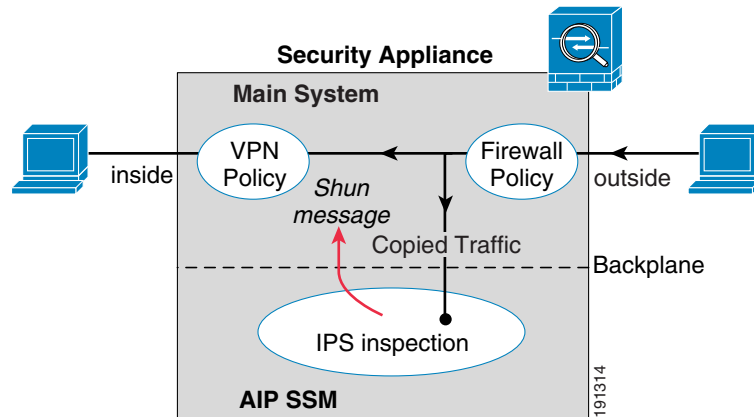
## Operating Modes

You can send traffic to the AIP SSM using one of the following modes:

- **Inline mode**—This mode places the AIP SSM directly in the traffic flow (see [Figure 28-1](#)). No traffic that you identified for IPS inspection can continue through the adaptive security appliance without first passing through, and being inspected by, the AIP SSM. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.

- Promiscuous mode—This mode sends a duplicate stream of traffic to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the AIP SSM can only block traffic by instructing the adaptive security appliance to shun the traffic or by resetting a connection on the adaptive security appliance. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the adaptive security appliance before the AIP SSM can shun it. [Figure 28-2](#) shows the AIP SSM in promiscuous mode. In this example, the AIP SSM sends a shun message to the security appliance for traffic it identified as a threat.

**Figure 28-2** AIP SSM Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



## Using Virtual Sensors

The AIP SSM running IPS software Version 6.0 and later can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

[Figure 28-3](#) shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

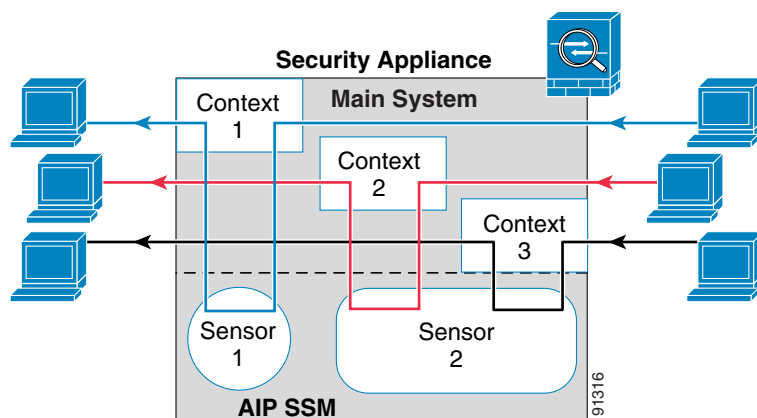
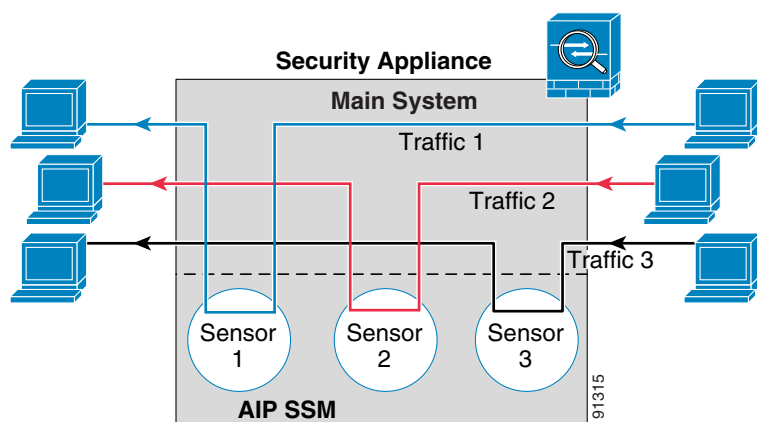
**Figure 28-3 Security Contexts and Virtual Sensors**

Figure 28-4 shows a single mode security appliance paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

**Figure 28-4 Single Mode Security Appliance with Multiple Virtual Sensors**

## AIP SSM Procedure Overview

Configuring the AIP SSM is a process that includes configuration of the AIP SSM and then configuration of the ASA 5500 series adaptive security appliance:

1. From ASDM, launch IDM. See the [“Accessing IDM from ASDM”](#) section on page 28-5. ASDM uses IDM to configure the AIP SSM.
2. In IDM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. Configure the inspection and protection policy for each virtual sensor if you want to run the AIP SSM in multiple sensor mode. See the [“Configuring the AIP SSM Security Policy in IDM”](#) section on page 28-5.
3. Using ASDM on the ASA 5500 series adaptive security appliance in multiple context mode, specify which IPS virtual sensors are available for each context (if you configured virtual sensors). See the [“Assigning Virtual Sensors to Security Contexts”](#) section on page 28-5.

4. Using ASDM on the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM. See the “[Diverting Traffic to the AIP SSM](#)” section on page 28-6.

## Accessing IDM from ASDM

ASDM uses IDM to configure the AIP SSM. If the AIP SSM is running IPS Version 6.0 or later, ASDM retrieves IDM from the AIP SSM and displays it as part of the ASDM interface. For earlier versions of the IPS software, IDM launches in a separate browser window.

To access IDM from ASDM, click **Configuration > IPS**.

You are asked for the IP address or hostname of the AIP SSM.

- If the AIP SSM is running IPS Version 6.0 or later, ASDM retrieves IDM from the AIP SSM and displays it as part of the ASDM interface. Enter the AIP SSM password and click **OK**.

The IDM panes appear in the ASDM window.

- If the AIP SSM is running an earlier version of IPS software, ASDM displays a link to IDM. Click the link to launch IDM in a new browser window. You need to provide a username and password to access IDM.

If the password to access IDM is lost, you can reset the password using ASDM. See the “[Resetting the AIP SSM Password](#)” section on page 28-8, for more information.

## Configuring the AIP SSM Security Policy in IDM

On the AIP SSM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. If you configure virtual sensors in IPS Version 6.0 or above, you identify one of the sensors as the default. If the ASA 5500 series adaptive security appliance does not specify a virtual sensor name in its configuration, the default sensor is used.

Because the IPS software that runs on the AIP SSM is beyond the scope of this document, detailed configuration information is available in the IDM online help. The IDM online help is available from the IDM panes displayed in ASDM. Additionally, you can see the IDM and IPS documentation on Cisco.com at the following location:

[http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html)

## Assigning Virtual Sensors to Security Contexts

If the security appliance is in multiple context mode, then you can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts.



### Note

You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

To assign one or more sensors to a security context, perform the following steps:

- 
- Step 1** In the ASDM Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Security Contexts pane, choose a context that you want to configure, and click **Edit**.
- The Edit Context dialog box appears. For more information about configuring contexts, see the [“Configuring Security Contexts” section on page 10-16](#).
- Step 3** In the IPS Sensor Allocation area, click **Add**.
- The IPS Sensor Selection dialog box appears.
- Step 4** From the Sensor Name drop-down list, choose a sensor name from those configured on the AIP SSM.
- Step 5** (Optional) To assign a mapped name to the sensor, enter a value in the Mapped Sensor Name field.
- This sensor name can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” sensors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
- Step 6** Click **OK** to return to the Edit Context dialog box.
- Step 7** (Optional) To set one sensor as the default sensor for this context, from the Default Sensor drop-down list, choose a sensor name.
- If you do not specify a sensor name when you configure IPS within the context configuration, the context uses this default sensor. You can only configure one default sensor per context. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.
- Step 8** Repeat this procedure for each security context.
- Step 9** Change to each context to configure the IPS security policy as described in [“Diverting Traffic to the AIP SSM” section on page 28-6](#).
- 

## Diverting Traffic to the AIP SSM

To identify traffic to divert from the adaptive security appliance to the AIP SSM, perform the following steps. In multiple context mode, perform these steps in each context execution space.

This feature is enabled using Service Policy rules. See [Chapter 22, “Configuring Service Policy Rules,”](#) for detailed information about creating a service policy.

- 
- Step 1** In the ASDM Device List pane, double-click the context name under the active device *IP address* > Contexts.
- Step 2** Click **Configuration > Firewall > Service Policy Rules**.
- Step 3** You can edit an existing rule or create a new one:
- For an existing rule, choose the rule and click **Edit**.  
The Edit Service Policy Rule dialog box appears.
  - For a new rule, choose **Add > Add Service Policy Rule**.



The Add Service Policy Rule Wizard - Service Policy dialog box appears. Complete the Service Policy and Traffic Classification Criteria dialog boxes. See the [“Adding a Service Policy Rule for Through Traffic”](#) section on page 22-6 for more information. Click **Next** to show the Add Service Policy Rule Wizard - Rule Actions dialog box.

**Step 4** Click the **Intrusion Prevention** tab.

You can also set other feature actions for the same traffic using the other tabs.

**Step 5** Check the **Enable IPS for this traffic flow** check box.

**Step 6** In the Mode area, click **Inline Mode** or **Promiscuous Mode**.

See the [“Operating Modes”](#) section on page 28-2 for more details.

**Step 7** In the If IPS Card Fails area, click **Permit traffic** or **Close traffic**.

The Close traffic option sets the adaptive security appliance to block all traffic if the AIP SSM is unavailable.

The Permit traffic option sets the adaptive security appliance to allow all traffic through, uninspected, if the AIP SSM is unavailable.

**Step 8** (Optional) From the IPS Sensor to use drop-down list, choose a virtual sensor name.

If you use virtual sensors on the AIP SSM, you can specify a sensor name using this option. If you use multiple context mode on the security appliance, you can only specify sensors that you assigned to the context (see the [“Assigning Virtual Sensors to Security Contexts”](#) section on page 28-5). If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM.

**Step 9** Click **OK**.

## Intrusion Prevention Tab Field Descriptions

### Fields

- **Enable IPS for this traffic flow**—Enables or disables intrusion prevention for this traffic flow. When this check box is checked, the other parameters on this window become active.
- **Mode**—Configures the operating mode for intrusion prevention. See the [“Operating Modes”](#) section on page 28-2 for more information.
  - **Inline Mode**—Selects Inline Mode, in which a packet is directed to IPS. The packet might be dropped as a result of the IPS operation.
  - **Promiscuous Mode**—Selects Promiscuous Mode, in which IPS operates on a duplicate of the original packet. The original packet cannot be dropped.
- **If IPS card fails**—Configures the action to take if the AIP SSM becomes inoperable.
  - **Permit traffic**—Permit traffic if the AIP SSM fails
  - **Close traffic**—Block traffic if the AIP SSM fails.
- **IPS Sensor Selection**—Selects the virtual sensor to use for this traffic flow. See the [“Using Virtual Sensors”](#) section on page 28-3 for more information.
  - **IPS Sensor to Use**—Sets a virtual sensor name. If you use virtual sensors on the AIP SSM, you can specify a sensor name using this option. If you use multiple context mode on the security appliance, you can only specify sensors that you assigned to the context (see the [“Assigning](#)

[Virtual Sensors to Security Contexts” section on page 28-5](#)). If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Resetting the AIP SSM Password

You can use ASDM to reset the AIP SSM password to the default if the AIP SSM is running IPS Version 6.0 or later. The default password is “cisco” (without the quotation marks). After resetting the password, you should change it to a unique value using IDM. See the [“Accessing IDM from ASDM” section on page 28-5](#) for information about accessing IDM from ASDM.

Resetting the AIP SSM password causes the AIP SSM to reboot. IPS services are not available while the AIP SSM is rebooting.

To reset the AIP SSM password to the default, perform the following steps:

- 
- Step 1** From the ASDM menu bar, choose **Tools > IPS Password Reset**.



**Note** This option does not appear in the menu if an SSM is not installed. This option appears as CSC Password Reset if a CSC SSM is installed.

---

The IPS Password Reset confirmation dialog box appears.

- Step 2** Click **OK** to reset the AIP SSM password to the default.

A dialog box displays the success or failure of the password reset. If the password was not reset, make sure you are using Version 7.2(2) or later of the platform software on the adaptive security appliance and IPS Version 6.0 or later on the AIP SSM.

- Step 3** Click **Close** to close the dialog box.
-



# CHAPTER 29

## Configuring Trend Micro Content Security



### Note

The ASA 5580 does not support the CSC SSM feature.

This chapter describes how to configure the CSC SSM, and includes the following sections:

- [Connecting to the CSC SSM, page 29-1](#)
- [Managing the CSC SSM, page 29-2](#)
- [CSC SSM Setup, page 29-7](#)
- [Web, page 29-19](#)
- [Mail, page 29-20](#)
- [File Transfer, page 29-22](#)
- [Updates, page 29-23](#)

## Connecting to the CSC SSM

With each session you start in ASDM, the first time you access features related to the CSC SSM, you must specify the management IP address and provide the password for the CSC SSM. After you successfully connect to the CSC SSM, you are not prompted again for the management IP address and password. If you start a new ASDM session, the connection to the CSC SSM is reset and you must specify the IP address and the CSC SSM password again. The connection to the CSC SSM is also reset if you change the time zone on the adaptive security appliance.



### Note

The CSC SSM has a password that is maintained separately from the ASDM password. You can configure the two passwords to be identical, but changing the CSC SSM password does not affect the ASDM password.

To connect to the CSC SSM, perform the following steps:

**Step 1** In the main ASDM application window, click the **Content Security** tab.

**Step 2** In the Connecting to CSC dialog box, choose one of the following options:

- **Management IP Address**—Connects to the IP address of the management port on the SSM. ASDM automatically detects the IP address for the SSM in the adaptive security appliance. If this detection fails, you can specify the management IP address manually.

- Other IP Address or Hostname—Connects to an alternate IP address or hostname on the SSM.

**Step 3** Enter the port number in the Port field, and then click **Continue**.

**Step 4** In the CSC Password dialog box, type your CSC password, and then click **OK**.



**Note** If you have not completed the CSC Setup Wizard (choose **Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup**), complete the configuration in the CSC Setup Wizard, which includes changing the default password, “cisco.”

For ten minutes after you have entered the password, you do not need to reenter the CSC SSM password to access other parts of the CSC SSM GUI.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Managing the CSC SSM

This section describes how to manage the CSC SSM, and includes the following topics:

- [About the CSC SSM, page 29-2](#)
- [Getting Started with the CSC SSM, page 29-3](#)
- [Determining What Traffic to Scan, page 29-5](#)
- [Rule Actions for CSC Scanning, page 29-6](#)

## About the CSC SSM

ASDM lets you configure activation codes and other, basic operational parameters for the Content Security and Control (CSC) SSM, as well as CSC-related features. The ASA 5500 series adaptive security appliance supports the CSC SSM, which runs content security and control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure on the adaptive security appliance to send to it.

[Figure 29-1](#) illustrates the flow of traffic through an adaptive security appliance that has the following:

- A CSC SSM installed and configured.

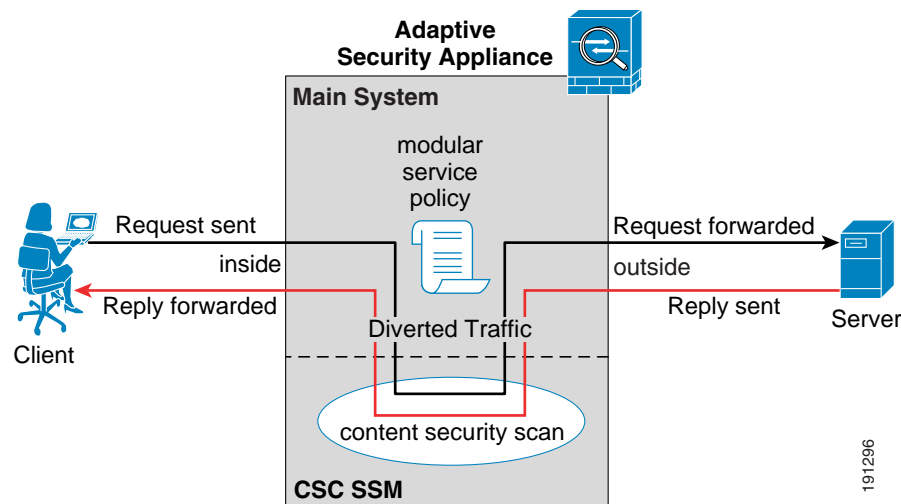
- A service policy that determines which traffic is diverted to the SSM for scans.

In this example, the client could be a network user who is accessing a website, downloading files from an FTP server, or retrieving e-mail from a POP3 server. SMTP scans differ in that you should configure the adaptive security appliance to scan traffic sent from outside to SMTP servers protected by the adaptive security appliance.

**Note**

The CSC SSM can scan FTP file transfers only when FTP inspection is enabled on the adaptive security appliance. By default, FTP inspection is enabled.

**Figure 29-1** Flow of Scanned Traffic with CSC SSM



You use ASDM for system setup and monitoring of the CSC SSM. To configure content security policies in the CSC SSM software, you click links within ASDM to access the web-based GUI for the CSC SSM. The CSC SSM GUI appears in a separate web browser window. To access the CSC SSM, you must enter the CSC SSM password. To use the CSC SSM GUI, see the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

**Note**

ASDM and the CSC SSM maintain separate passwords. You can configure their passwords to be identical; however, changing one of these two passwords does not affect the other password.

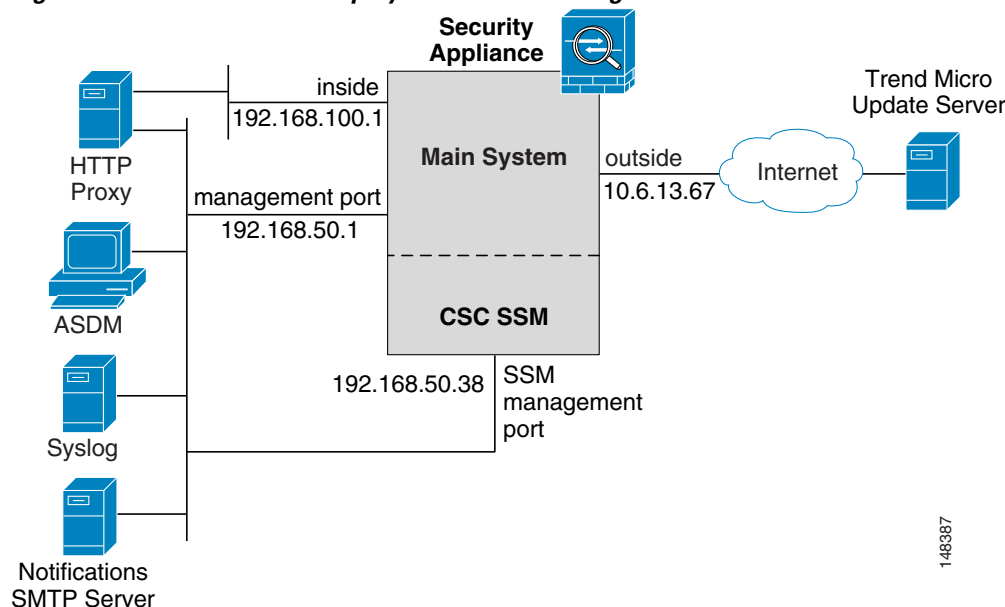
The connection between the host running ASDM and the adaptive security appliance is made through a management port on the adaptive security appliance. The connection to the CSC SSM GUI is made through the SSM management port. Because these two connections are required to manage the CSC SSM, any host running ASDM must be able to reach the IP address of both the adaptive security appliance management port and the SSM management port.

Figure 29-2 shows an adaptive security appliance with a CSC SSM that is connected to a dedicated management network. Although a dedicated management network is not required, we recommend that you use one. This figure includes the following:

- An HTTP proxy server is connected to the inside network and to the management network to enable the CSC SSM to contact the Trend Micro Update Server.

- The management port of the adaptive security appliance is connected to the management network. To allow management of the adaptive security appliance and the CSC SSM, hosts running ASDM must be connected to the management network.
- The management network includes an SMTP server for e-mail notifications for the CSC SSM and a syslog server to which the CSC SSM can send system log messages.

**Figure 29-2** CSC SSM Deployment with a Management Network



## Getting Started with the CSC SSM

Before you receive the security benefits that by a CSC SSM provides, you must perform several steps in addition to SSM hardware installation.

To configure the adaptive security appliance and the CSC SSM, perform the following steps:

- Step 1** If the CSC SSM was not pre-installed in a Cisco ASA 5500 series adaptive security appliance, install the CSC SSM and connect a network cable to the SSM management port. For assistance with SSM installation and connection, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

The CSC SSM management port must be connected to your network to allow management of and automatic updates to the CSC SSM software. Additionally, the CSC SSM uses the management port for e-mail notifications and syslog message generation.

- Step 2** With the CSC SSM, you received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL:

<http://www.cisco.com/go/license>

After you register, you will receive activation keys by e-mail. The activation keys are required before you can complete [Step 5](#).

- Step 3** Obtain the following information, for use in [Step 5](#).

- Activation keys, received after completing [Step 2](#).
- The SSM management port IP address, netmask, and gateway IP address. The SSM management port IP address must be accessible by the hosts used to run ASDM. The IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.
- DNS server IP address.
- HTTP proxy server IP address (necessary only if your security policies require use of a proxy server for HTTP access to the Internet).
- Domain name and hostname for the SSM.
- An e-mail address and an SMTP server IP address and port number, for e-mail notifications.
- IP addresses of hosts or networks that are allowed to manage the CSC SSM.
- Password for the CSC SSM.

**Step 4** In ASDM, verify time settings on the security appliance. Time setting accuracy is important for logging of security events and for automatic updates of the CSC SSM software.

- If you manually control time settings, verify the clock settings, including time zone. Choose **Configuration > > Device Setup > System Time > Clock**.
- If you are using NTP, verify the NTP configuration. Choose **Configuration > Device Setup > System Time > NTP**.

**Step 5** Complete the CSC Setup Wizard.

- Choose **Configuration > Trend Micro Content Security**. Connect to and log in to the CSC SSM. Choose **CSC Setup > Wizard Setup**, and then click **Launch Setup Wizard**.
- If you are rerunning the CSC Setup Wizard, perform the same steps listed in the previous bullet:

For assistance with the CSC Setup Wizard, click **Help**.

**Step 6** Configure service policies to divert to the CSC SSM the traffic that you want scanned.

If you create a global policy to divert traffic for scans, all traffic (inbound and outbound) for the supported protocols is scanned. To maximize performance of the adaptive security appliance and the CSC SSM, scan traffic only from untrusted sources.

To view best practices for diverting traffic to the CSC SSM, see [Determining What Traffic to Scan, page 29-5](#).

If you want to create a global policy that diverts traffic for scans, perform the following steps:

- Choose **Configuration > Firewall > Service Policy Rules**, and then click **Add**.  
The Add Service Policy Rule Wizard screen appears.
- Click the **Global - applies to all interfaces** option, and then click **Next**.  
The Traffic Classification Criteria screen appears.
- Click the **Create a new traffic class** option, type a name for the traffic class in the adjacent field, check the **Any traffic** check box, and then click **Next**.  
The Rule Actions screen appears.
- Click the **CSC Scan** tab, and then check the **Enable CSC scan for this traffic flow** check box.
- Choose whether the adaptive security appliance should permit or deny selected traffic to pass if the CSC SSM is unavailable by making the applicable selection in the area labeled: **If CSC card fails, then**.
- Click **Finish**.

The new service policy appears in the Service Policy Rules pane.

**g. Click **Apply**.**

The adaptive security appliance begins diverting traffic to the CSC SSM, which performs the content security scans that have been enabled according to the license that you purchased.

**Step 7** (Optional) Review the default content security policies in the CSC SSM GUI. The default content security policies are suitable for most implementations. Modifying them requires advanced configuration that you should perform only after reading the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.



**Note**

You review the content security policies by viewing the enabled features in the CSC SSM GUI. The availability of features depends on the license that you purchased. By default, all features included in the license that you purchased are enabled.

With a Base License, the features enabled by default are SMTP virus scanning, POP3 virus scanning and content filtering, webmail virus scanning, HTTP file blocking, FTP virus scanning and file blocking, logging, and automatic updates.

With a Plus License, the additional features enabled by default are SMTP anti-spam, SMTP content filtering, POP3 anti-spam, URL blocking, and URL filtering.

To access the CSC SSM GUI in ASDM, choose **Configuration > Trend Micro Content Security**, and then click one of the following links: **Web**, **Mail**, **File Transfer**, or **Updates**. To open the CSC SSM GUI, click one of the links in these panes.

## Determining What Traffic to Scan

The CSC SSM can scan FTP, HTTP, POP3, and SMTP traffic; however, it supports these protocols only when the destination port of the packet requesting the connection is the established port for the protocol. The CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21.
- HTTP connections opened to TCP port 80.
- POP3 connections opened to TCP port 110.
- SMTP connections opened to TCP port 25.

You can choose to scan traffic for all of these protocols or any combination of them. For example, if you do not allow network users to receive POP3 e-mail, you would not want to configure the adaptive security appliance to divert POP3 traffic to the CSC SSM. You would want to block POP3 traffic instead.

To maximize performance of the adaptive security appliance and the CSC SSM, divert to the CSC SSM only the traffic that you want the CSC SSM to scan. Diverting traffic that you do not want to scan, such as traffic between a trusted source and destination, can adversely affect network performance.



**Note**

When traffic is first classified for CSC inspection, it is flow-based. If traffic is part of a pre-existing connection, the traffic goes directly to the policy set for that connection.



You enable traffic scanning with the CSC SSM on the CSC Scan tab in the Add Service Policy Rule Wizard Rule Actions screen. You can apply service policies that include CSC scanning globally or to specific interfaces; therefore, you can choose to enable CSC scans globally or for specific interfaces. For more information, see [Rule Actions for CSC Scanning, page 29-6](#).

Adding the `csc` command to your global policy ensures that all unencrypted connections through the adaptive security appliance are scanned by the CSC SSM; however, this setting may cause traffic from trusted sources to be scanned unnecessarily.

If you enable CSC scans in interface-specific service policies, these scans are bi-directional.

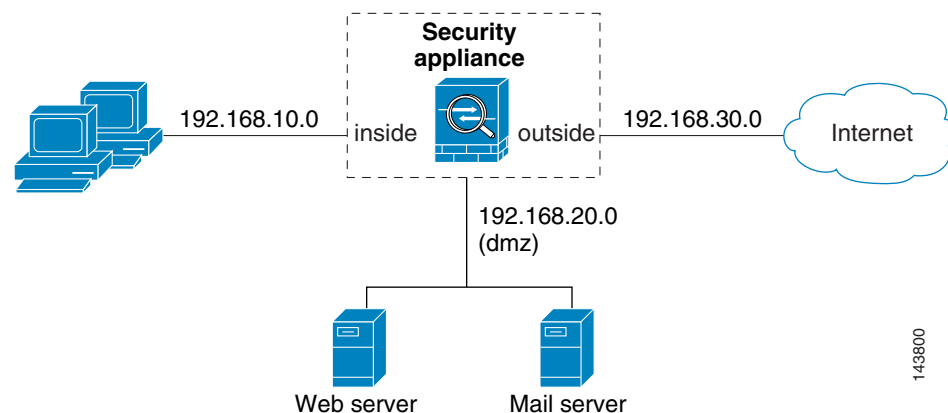
Bi-directional scanning means that when the adaptive security appliance opens a new connection, if CSC scanning is active on either the inbound or the outbound interface of that connection and the service policy identifies traffic for scanning, the adaptive security appliance diverts this traffic to the CSC SSM. Bi-directional scanning also means that if you divert any of the supported traffic types that cross a given interface to the CSC SSM, unnecessary scanning may be occurring on traffic from your trusted inside networks. For example, URLs and files requested from web servers on a DMZ network are unlikely to pose content security risks to hosts on an inside network, and you probably do not want the adaptive security appliance to divert such traffic to the CSC SSM.

Therefore, we highly recommend that the service policies to define CSC scans use access lists to limit the selected traffic. Specifically, use access lists that match the following:

- HTTP connections to outside networks.
- FTP connections from clients inside the adaptive security appliance to servers outside the adaptive security appliance.
- POP3 connections from clients inside the adaptive security appliance to servers outside the adaptive security appliance.
- Incoming SMTP connections destined to go to inside mail servers.

In [Figure 29-3](#), you should configure the adaptive security appliance to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. You should not enable scanning of HTTP requests from the inside network to the web server on the DMZ network.

**Figure 29-3 Common Network Configuration for CSC SSM Scanning**



There are many ways you could configure the adaptive security appliance to identify the traffic that you want to scan. One approach is to define two service policies: one on the inside interface and the other on the outside interface, each with access lists that match traffic to be scanned.

Figure 29-4 shows service policy rules that select only the traffic that the adaptive security appliance should scan.

**Figure 29-4** Optimized Traffic Selection for CSC Scans

| Traffic Classification                            |               |                                     |       |                 |                 |              |                | Rule Actions        |
|---------------------------------------------------|---------------|-------------------------------------|-------|-----------------|-----------------|--------------|----------------|---------------------|
| #                                                 | Name          | Enabled                             | Match | Source          | Destination     | Service      | Time           |                     |
| <b>Interface: inside, Policy: inside-policy</b>   |               |                                     |       |                 |                 |              |                |                     |
| 1                                                 | inside-class1 | <input checked="" type="checkbox"/> |       | 192.168.10.0/24 | 192.168.20.0/24 | tcp www/tcp  | -- Not Appl... | csc, permit traffic |
| 1                                                 | inside-class  | <input checked="" type="checkbox"/> |       | 192.168.10.0/24 | any             | tcp ftp/tcp  | -- Not Appl... | csc, permit traffic |
| 2                                                 |               | <input checked="" type="checkbox"/> |       | 192.168.10.0/24 | any             | tcp www/tcp  | -- Not Appl... |                     |
| 3                                                 |               | <input checked="" type="checkbox"/> |       | 192.168.10.0/24 | any             | tcp pop3/tcp | -- Not Appl... |                     |
| <b>Interface: outside, Policy: outside-policy</b> |               |                                     |       |                 |                 |              |                |                     |
| 1                                                 | outside-class | <input checked="" type="checkbox"/> |       | any             | 192.168.20.0/24 | tcp smtp/tcp | -- Not Appl... | csc, permit traffic |

In the inside-policy, the first class, inside-class1, ensures that the adaptive security appliance does not scan HTTP traffic between the inside network and the DMZ network. The Match column indicates this setting by displaying the “Do not match” icon. This setting does not mean the adaptive security appliance blocks traffic sent from the 192.168.10.0 network to TCP port 80 on the 192.168.20.0 network. Instead, this setting exempts the traffic from being matched by the service policy applied to the inside interface, which prevents the adaptive security appliance from sending the traffic to the CSC SSM.

The second class of the inside-policy, inside-class matches FTP, HTTP, and POP3 traffic between the inside network and any destination. HTTP connections to the DMZ network are exempted because of the inside-class1 setting. As previously mentioned, policies that apply CSC scanning to a specific interface affect both incoming and outgoing traffic, but by specifying 192.168.10.0 as the source network, inside-class1 matches only connections initiated by the hosts on the inside network.

In the outside-policy, outside-class matches SMTP traffic from any outside source to the DMZ network. This setting protects the SMTP server and inside users who download e-mail from the SMTP server on the DMZ network, without having to scan connections from SMTP clients to the server.

If the web server on the DMZ network receives files uploaded by HTTP from external hosts, you can add a rule to the outside policy that matches HTTP traffic from any source to the DMZ network. Because the policy is applied to the outside interface, the rule would only match connections from HTTP clients outside the adaptive security appliance.

## Rule Actions for CSC Scanning

The CSC Scan tab lets you determine whether the CSC SSM scans traffic identified by the current traffic class. This tab appears only if a CSC SSM is installed in the adaptive security appliance.

The CSC SSM scans only HTTP, SMTP, POP3, and FTP traffic. If your service policy includes traffic that supports other protocols in addition to these four, packets for other protocols are passed through the CSC SSM without being scanned. To reduce the load on the CSC SSM, configure the service policy rules that send packets to the CSC SSM to support only HTTP, SMTP, POP3, or FTP traffic.

### Fields

- Enable CSC scan for this traffic flow—Enables or disables use of the CSC SSM for this traffic flow. When this check box is checked, the other parameters on this tab become active.

- If CSC card fails—Configures the action to take if the CSC SSM becomes inoperable.
  - Permit traffic—Allows traffic if the CSC SSM fails.
  - Close traffic—Blocks traffic if the CSC SSM fails.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## CSC SSM Setup

The screens under CSC Setup let you configure basic operational parameters for the CSC SSM. You must complete the CSC Setup Wizard at least once before you can configure each screen separately. After you complete the CSC Setup Wizard, you can modify each screen individually without using this wizard again.

Additionally, you cannot access the panes under Home > Trend Micro Content Security > Content Security Tab or Monitoring > Trend Micro Content Security > Content Security Tab until you complete the CSC Setup Wizard. If you try to access these panes before completing this wizard, a dialog box appears and lets you access the wizard directly to complete the configuration.

For an introduction to the CSC SSM, see [About the CSC SSM, page 29-2](#). For more information, see the following topics:

- [Activation/License, page 29-8](#)
- [IP Configuration, page 29-9](#)
- [Host/Notification Settings, page 29-9](#)
- [Management Access Host/Networks, page 29-10](#)
- [Password, page 29-11](#)
- [Restoring the Default Password, page 29-12](#)
- [Wizard Setup, page 29-13](#)

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the panes under the CSC Setup node are available only in the admin context.

#### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Activation/License

The Activation/License pane lets you configure activation codes for the following two components of the CSC SSM:

- Base License
- Plus License

You can use ASDM to configure CSC licenses only once each for the two licenses. Renewed license activation codes are downloaded automatically with scheduled software updates. Links to the licensing status page and the CSC UI home page appear at the bottom of this window. The serial number for the assigned license is filled in automatically.

#### Fields

- Product—*Display only*. Shows the name of the component.
- Activation Code—Contains the activation code for the corresponding Product field.
- License Status—*Display only*. Shows information about the status of the license. If the license is valid, the expiration date appears. If expiration date has passed, this field indicates that the license has expired.
- Nodes—*Display only*. Shows the maximum number of network devices supported by the Base License of your CSC SSM. The Plus License does not affect the number of network devices supported; therefore, the Nodes field does not appear in the Plus License area.
- Click the link provided to review license status or renew your license.
- Click the link provided to go to the CSC home page in ASDM.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the Activation/License pane is available only in the admin context.

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## IP Configuration

The IP Configuration pane lets you configure IP addresses and other relevant details for the CSC SSM, the DNS servers it should use, and a proxy server for retrieving CSC SSM software updates.

**Fields**

- **Management Interface**—Contains parameters for management access to the CSC SSM.
  - **IP Address**—Sets the IP address for management access to the CSC SSM.
  - **Mask**—Sets the netmask for the network containing the management IP address of the CSC SSM.
  - **Gateway**—Sets the IP address of the gateway device for the network that contains the management IP address of the CSC SSM.
- **DNS Servers**—Contains parameters about DNS servers for the network containing the management IP address of the CSC SSM.
  - **Primary DNS**—Sets the IP address of the primary DNS server.
  - **Secondary DNS**—(Optional) Sets the IP address of the secondary DNS server.
- **Proxy Server**—Contains parameters for an optional HTTP proxy server, used by the CSC SSM to contact a CSC SSM software update server. If your network configuration does not require the CSC SSM to use a proxy server, you can leave the fields in this group blank.
  - **Proxy Server**—(Optional) Sets the IP address of the proxy server.
  - **Proxy Port**—(Optional) Sets the listening port of the proxy server.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the IP Configuration pane is available only in the admin context.

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## Host/Notification Settings

The Host/Notification Settings pane lets you configure details about hostname, domain name, e-mail notifications, and a domain name for e-mails to be excluded from detailed scanning.

### Fields

- **Host and Domain Names**—Contains information about the hostname and domain name of the CSC SSM.
  - **HostName**—Sets the hostname of the CSC SSM.
  - **Domain Name**—Sets the domain name that contains the CSC SSM.
- **Incoming E-mail Domain Name**—Contains information about a trusted incoming e-mail domain name for SMTP-based e-mail.
  - **Incoming Email Domain**—Sets the incoming e-mail domain name. The CSC SSM scans SMTP e-mail sent to this domain. The types of threats that the CSC SSM scans for depend on the license that you purchased for the CSC SSM and the configuration of the CSC SSM software.



#### Note

CSC SSM lets you configure a list of many incoming e-mail domains. ASDM displays only the first domain in the list. To configure additional incoming e-mail domains, access the CSC SSM interface. To do so, choose **Configuration > Trend Micro Content Security > Email**, and then click one of the links. After logging in to the CSC SSM, choose **Mail (SMTP) > Configuration**, and then click the **Incoming Mail** tab.

- **Notification Settings**—Contains information required for e-mail notification of events.
  - **Administrator Email**—Sets the e-mail address for the account to which notification e-mails should be sent.
  - **Email Server IP Address**—Sets the IP address of the SMTP server.
  - **Port**—Sets the port to which the SMTP server listens.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the Host/Notification Settings pane is available only in the admin context.

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Management Access Host/Networks

The Management Access Host/Networks pane lets you control the hosts and networks from which management access to the CSC SSM is permitted. You must specify at least one permitted host or network. You can specify a maximum of eight permitted hosts or networks.

### Fields

- **IP Address**—Sets the address of a host or network you want to add to the Selected Hosts/Network list.
- **Mask**—Sets the netmask for the host or network you specified in the IP Address field.  
To allow all hosts and networks, enter **0.0.0.0** in the IP Address field and choose **0.0.0.0** from the Mask list.
- **Selected Hosts/Networks**—Displays the hosts or networks trusted for management access to the CSC SSM. ASDM requires that you configure at least one host or network. You can configure a maximum of eight hosts or networks.  
To remove a host or network from the list, choose its entry in the list and click **Delete**.
- **Add**—Adds the host or network you specified in the IP Address field to the Selected Hosts/Networks list.
- **Delete**—Removes the host or network selected in the Selected Hosts/Networks list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | • 1      | —      |

1. In multiple-context mode, the Management Access Host/Networks pane is available only in the admin context.

### For More Information

[Managing the CSC SSM, page 29-2](#)

## Password

The Password pane lets you change the password required for management access to the CSC SSM. The CSC SSM has a password that is maintained separately from the ASDM password. You can configure them to be identical; however, changing the CSC SSM password does not affect the ASDM password.

If ASDM is connected to the CSC SSM and you change the CSC SSM password, the connection to the CSC SSM is dropped. As a result, ASDM displays a confirmation dialog box that you must respond to before the password is changed.



#### Tip

Whenever the connection to the CSC SSM is dropped, you can reestablish it. To do so, click the **Connection to Device** icon on the status bar to display the Connection to Device dialog box, and then click **Reconnect**. ASDM prompts you for the CSC SSM password, which is the new password that you have defined.

Passwords must be 5 - 32 characters long.

Passwords appears as asterisks when you type them.

**Note**

The default password is “cisco.”

**Fields**

- Old Password—Requires the current password for management access to the CSC SSM.
- New Password—Sets the new password for management access to the CSC SSM.
- Confirm New Password—Verifies the new password for management access to the CSC SSM.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the Password pane is available only in the admin context.

**For More Information**

[Managing the CSC SSM, page 29-2](#)

## Restoring the Default Password

You can use ASDM to reset the CSC SSM password. You can reset this password to the default value, which is “cisco” (excluding quotation marks). If the CSC password-reset policy has been set to “Denied,” then you cannot reset the password through the ASDM CLI. To change this policy, you must session in to the CSC SSM. For more information, see the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

**Note**

This option does not appear in the menu if an SSM is not installed.

To reset the CSC SSM password to the default value, perform the following steps:

- 
- Step 1** From the ASDM menu bar, choose **Tools > CSC Password Reset**.  
The CSC Password Reset confirmation dialog box appears.
- Step 2** Click **OK** to reset the CSC SSM password to the default value.  
A dialog box appears, indicating the success or failure of the password reset. If the password was not reset, make sure you are using Version 8.0(2) software on the adaptive security appliance and the most recent Version 6.1.x software on the CSC SSM.
- Step 3** Click **Close** to close the dialog box.
- Step 4** After you have reset the password, you should change it to a unique value.
-



**Note**

This feature is available only in multiple-context mode in the system context.

**For More Information**

See [Password](#), page 29-11

## Wizard Setup

The Wizard Setup screen lets you start the CSC Setup Wizard.

Before you can directly access any of the other screens under CSC Setup, you must complete the CSC Setup Wizard. This wizard includes the following screens:

- [CSC Setup Wizard Activation Codes Configuration](#), page 29-13
- [CSC Setup Wizard IP Configuration](#), page 29-14
- [CSC Setup Wizard Host Configuration](#), page 29-15
- [CSC Setup Wizard Management Access Configuration](#), page 29-15
- [CSC Setup Wizard Password Configuration](#), page 29-16
- [CSC Setup Wizard Traffic Selection for CSC Scan](#), page 29-16
- [CSC Setup Wizard Summary](#), page 29-18

After you complete the CSC Setup Wizard, you can change any settings in screens related to the CSC SSM without using the CSC Setup Wizard again.

**Fields**

- Launch Setup Wizard—Click to start the CSC Setup Wizard.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |                |        |
|---------------|-------------|------------------|----------------|--------|
| Routed        | Transparent | Single           | Multiple       |        |
|               |             |                  | Context        | System |
| •             | •           | •                | • <sup>1</sup> | —      |

1. In multiple-context mode, the Wizard Setup screen is available only in the admin context.

**For More Information**

See [Managing the CSC SSM](#), page 29-2

## CSC Setup Wizard Activation Codes Configuration

The CSC Setup Wizard Activation Codes Configuration screen displays the activation codes that you have entered to enable features on the CSC SSM, according to the type of license you have.

**Fields**

- Activation Code—*Display only*. Displays the activation code settings you have made on this screen.
  - Base License—Shows the activation code. The Base License includes anti-virus, anti-spyware, and file blocking.
  - Plus License—Shows the activation code, if you have entered one. If not, this field is blank. The Plus License includes anti-spam, anti-phishing, content filtering, and URL blocking and filtering.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## CSC Setup Wizard IP Configuration

The CSC Setup Wizard IP Configuration screen displays the IP configuration settings that you have entered for the CSC SSM.

**Fields**

- IP Address—Shows the IP address for the management interface of the CSC SSM.
- Mask—Shows the network mask for the management interface of the CSC SSM that you have selected from the drop-down list.
- Gateway—Shows the IP address of the gateway device for the network that contains the CSC SSM management interface.
- Primary DNS— Shows the primary DNS server IP address.
- Secondary DNS (optional)—Shows the secondary DNS server IP address (if configured).
- Proxy Server (optional)—Shows the proxy server (if configured).
- Proxy Port (optional)—Shows the proxy port (if configured).

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## CSC Setup Wizard Host Configuration

The CSC Setup Wizard Host Configuration screen displays the host and domain names, incoming e-mail domain name, administrator e-mail address, e-mail server IP address, and the port number that you have entered for the CSC SSM.

**Fields**

- **Hostname**—Shows the hostname of the CSC SSM.
- **Domain Name**—Shows the name of the domain in which the CSC SSM resides.
- **Incoming Email Domain**—Shows the domain name for incoming e-mail.
- **Administrator E-mail**—Shows the e-mail address of the domain administrator.
- **E-mail Server IP Address**—Shows the IP address of the e-mail server.
- **Port**—Shows the port number through which you connect to the CSC SSM.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM](#)

## CSC Setup Wizard Management Access Configuration

The CSC Setup Wizard IP Configuration screen displays the subnet and host settings that you have entered to grant access to the CSC SSM.

**Fields**

- **IP Address**—Shows the IP address for networks and hosts that are allowed to connect to the CSC SSM.
- **Mask**—Shows the network mask for networks and hosts that are allowed to connect to the CSC SSM that you have selected from the drop-down list.
- **Add**—Click to add the IP address of the networks and hosts that you want to allow to connect to the CSC SSM.
- **Delete**—Click to remove the IP address of a network or host whose ability to connect to the CSC SSM you no longer want.
- **Selected Hosts/Networks**—Lists the IP addresses of networks and hosts whose connection to the CSC SSM you have added.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## CSC Setup Wizard Password Configuration

The CSC Setup Wizard Password Configuration screen displays the password settings that you have entered to grant access to the CSC SSM.

**Fields**

- Old Password—Requires the current password to access the CSC SSM.
- New Password—Sets the new password to access the CSC SSM.
- Confirm New Password—Verifies the new password to access the CSC SSM.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## CSC Setup Wizard Traffic Selection for CSC Scan

The CSC Setup Wizard Traffic Selection for CSC Scan screen displays the settings that you have made to select traffic for CSC scanning.

**Fields**

- Interface—Specifies the interface to the CSC SSM that you have chosen from the drop-down list.
- Source—Specifies the source of network traffic for the CSC SSM to scan.
- Destination—Specifies the destination of network traffic for the CSC SSM to scan.
- Service—Specifies the source or destination service for the CSC SSM to scan.

- **Add**—Click to specify additional traffic details for CSC scanning. For more information, see [Specify traffic for CSC Scan, page 29-17](#).
- **Edit**—Click to modify additional traffic details for CSC scanning. For more information, see [Specify traffic for CSC Scan, page 29-17](#).
- **Delete**—Click to remove additional traffic details for CSC scanning.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Specify traffic for CSC Scan

The Specify traffic for CSC Scan dialog box allows you to define, modify, or remove additional settings for selecting traffic for CSC scanning.

### Fields

- **Interface**—Choose the type of interface to the CSC SSM from the drop-down list. Available settings are global (all interfaces), inside, management, and outside.
- **Source**—Choose the source of network traffic for the CSC SSM to scan from the drop-down list.
- **Destination**—Choose the destination of network traffic for the CSC SSM to scan from the drop-down list.
- **Service**—Choose the type of service for the CSC SSM to scan from the drop-down list.
- **Description**—Describes the network traffic that you define for the CSC SSM to scan.
- **If CSC card fails**—Specifies whether or not to allow the CSC SSM to scan network traffic if the CSC card fails.

Click **Permit** to allow traffic through without being scanned. Click **Close** to prevent traffic from going through without being scanned. Click **OK** to save your settings. The added traffic details appear on the CSC Setup Wizard Traffic selection for CSC Scan screen. Click **Cancel** to discard these settings and return to the CSC Setup Wizard Traffic selection for CSC Scan screen. If you click **Cancel**, ASDM displays a dialog box to confirm your decision.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [CSC Setup Wizard Traffic Selection for CSC Scan, page 29-16](#)

## CSC Setup Wizard Summary

The CSC Setup Wizard Summary screen displays the settings that you have made with the CSC Setup Wizard. You can review your selections before you exit the wizard. If you want to change any of the settings, you can click **Back** to return to the previous screens that include those settings, make the needed changes, and click **Next** to return to this screen.

**Note**

After you click **Finish**, you can change any settings related to the CSC SSM without using the CSC Setup Wizard again.

**Fields**

- Activation Codes—*Display only*. Summarizes the settings that you made in the Activation Codes Configuration screen.
  - Base—Shows the Base License activation code.
  - Plus—Shows the Plus License activation code, if you entered one. If not, this field is blank.
- IP Parameters—*Display only*. Summarizes the settings that you made in the IP Configuration screen, including the following information:
  - IP address and netmask for the management interface of the CSC SSM.
  - IP address of the gateway device for the network that includes the CSC SSM management interface.
  - Primary DNS server IP address.
  - Secondary DNS server IP address (if configured).
  - Proxy server and port (if configured).
- Host and Domain Names—*Display only*. Summarizes the settings that you made in the Host Configuration screen, including the following information:
  - Hostname of the CSC SSM.
  - Domain name for the domain that includes the CSC SSM.
  - Domain name for incoming e-mail.
  - Administrator e-mail address.
  - E-mail server IP address and port number.
- Management Access List—Summarizes the settings that you have made on the Management Access Configuration screen. The drop-down list includes the hosts and networks from which the CSC SSM will allow management connections.

- Password—*Display only*. Indicates whether or not you have changed the password in the Password Configuration screen.
- Back—Click to return to preceding screens of the CSC Setup Wizard.
- Next—Dimmed; however, if you click **Back** to access any of the preceding screens in this wizard, click **Next** to return to this screen.
- Finish—Completes the CSC Setup Wizard and saves all settings that you have specified.
- Cancel—Exits the CSC Setup Wizard without saving any of the selected settings. If you click **Cancel**, ASDM displays a dialog box to confirm your decision.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Web

The Web pane lets you view whether or not web-related features are enabled and lets you access the CSC SSM for configuring these features.



### Note

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

### Fields

- URL Blocking and Filtering—Includes information and links related to URL blocking and filtering.
  - URL Blocking—*Display only*. Shows whether or not URL blocking is enabled on the CSC SSM.
  - Configure URL Blocking—Opens a screen for configuring URL blocking on the CSC SSM.
  - URL Filtering—*Display only*. Shows whether or not URL filtering is enabled on the CSC SSM.
  - Configure URL Filtering Rules—Opens a screen for configuring URL filtering rules on the CSC SSM.
  - Configure URL Filtering Settings—Opens a screen for configuring settings for URL filtering on the CSC SSM.
- File Blocking—Includes a field and a link about HTTP file blocking on the CSC SSM.
  - File Blocking—*Display only*. Shows whether or not file blocking is enabled on the CSC SSM.
  - Configure File Blocking—Opens a screen for configuring HTTP file blocking settings on the CSC SSM.

- Scanning—Includes a field and a link about HTTP scanning on the CSC SSM.
  - HTTP Scanning—*Display only*. Shows whether or not HTTP scanning is enabled on the CSC SSM.
  - Configure Web Scanning—Opens a screen for configuring HTTP scanning on the CSC SSM.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Mail

The Mail pane lets you see whether or not e-mail-related features are enabled and lets you access the CSC SSM to configure these features.

For more information about configuring these areas, see the following topics:

- [SMTP Tab, page 29-20](#)
- [POP3 Tab, page 29-21](#)

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## SMTP Tab

The SMTP tab displays fields and links specific to SMTP e-mail features on the CSC SSM.



### Note

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.



**Fields**

- Scanning—Includes fields and links about SMTP scanning.
  - Incoming Scan—*Display only*. Shows whether or not the incoming SMTP scanning feature is enabled on the CSC SSM.
  - Configure Incoming Scan—Opens a screen for configuring incoming SMTP scan settings on the CSC SSM.
  - Outgoing Scan—*Display only*. Shows whether or not the outgoing SMTP scanning feature is enabled on the CSC SSM.
  - Configure Outgoing Scan—Opens a screen for configuring outgoing SMTP scan settings on the CSC SSM.
- Content Filtering—Includes fields and links about SMTP content filtering.
  - Incoming Filtering—*Display only*. Shows whether or not content filtering for incoming SMTP e-mail is enabled on the CSC SSM.
  - Configure Incoming Filtering—Opens a screen for configuring incoming SMTP content filtering settings on the CSC SSM.
  - Outgoing Filtering—*Display only*. Shows whether or not content filtering for outgoing SMTP e-mail is enabled on the CSC SSM.
  - Configure Outgoing Filtering—Opens a screen for configuring outgoing SMTP content filtering settings on the CSC SSM.
- Anti-spam—Includes fields and links about the SMTP anti-spam feature.
  - Spam Prevention—*Display only*. Shows whether or not the SMTP anti-spam feature is enabled on the CSC SSM.
  - Configure Anti-spam—Opens a screen for configuring SMTP anti-spam settings on the CSC SSM.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

## POP3 Tab

The POP3 tab displays fields and links specific to POP3 e-mail features on the CSC SSM.



**Note**

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

**Fields**

- Scanning—*Display only*. Shows whether or not POP3 e-mail scanning is enabled on the CSC SSM.
- Configure Scanning—Opens a screen for configuring POP3 e-mail scanning on the CSC SSM.
- Anti-spam—*Display only*. Shows whether or not the POP3 anti-spam feature is enabled on the CSC SSM.
- Configure Anti-spam—Opens a screen for configuring the POP3 anti-spam feature on the CSC SSM.
- Content Filtering—*Display only*. Shows whether or not POP3 e-mail content filtering is enabled on the CSC SSM.
- Configure Content Filtering—Opens a screen for configuring POP3 e-mail content filtering on the CSC SSM.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)

# File Transfer

The File Transfer pane lets you view whether or not FTP-related features are enabled and lets you access the CSC SSM for configuring FTP-related features.



**Note**

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

**Fields**

- File Scanning—*Display only*. Shows whether or not FTP file scanning is enabled on the CSC SSM.
- Configure File Scanning—Opens a screen for configuring FTP file scanning settings on the CSC SSM.
- File Blocking—*Display only*. Shows whether or not FTP file blocking is enabled on the CSC SSM.

- **Configure File Blocking**—Opens a screen for configuring FTP file blocking settings on the CSC SSM.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

### For More Information

See [Managing the CSC SSM, page 29-2](#)

## Updates

The Updates pane lets you view whether or not scheduled updates are enabled and lets you access the CSC SSM for configuring scheduled updates.



### Note

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

### Fields

- **Scheduled Updates**—*Display only*. Shows whether or not scheduled updates are enabled on the CSC SSM.
- **Scheduled Update Frequency**—Displays information about when updates are scheduled to occur, such as “Hourly at 10 minutes past the hour.”
- **Component**—Displays names of parts of the CSC SSM software that can be updated.
- **Scheduled Updates**—*Display only*. Shows whether or not scheduled updates are enabled for the corresponding components.
- **Configure Updates**—Opens a window for configuring scheduled update settings on the CSC SSM.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

**For More Information**

See [Managing the CSC SSM, page 29-2](#)



## CHAPTER 30

# Configuring ARP Inspection and Bridging Parameters

---

This chapter describes how to enable ARP inspection and how to customize bridging operations for the security appliance in transparent firewall mode. In multiple context mode, the commands in this chapter can be entered in a security context, but not the system.

For information about transparent firewall mode, see [Chapter 18, “Firewall Mode Overview.”](#)

This chapter includes the following sections:

- [Configuring ARP Inspection, page 30-1](#)
- [Customizing the MAC Address Table, page 30-4](#)

## Configuring ARP Inspection

This section describes ARP inspection and how to enable it, and includes the following topics:

- [ARP Inspection, page 30-1](#)
- [Edit ARP Inspection Entry, page 30-2](#)
- [ARP Static Table, page 30-3](#)
- [Add/Edit ARP Static Configuration, page 30-4](#)

## ARP Inspection

The ARP Inspection pane lets you configure ARP inspection.

By default, all ARP packets are allowed through the security appliance. You can control the flow of ARP packets by enabling ARP inspection.

When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.

**Note**

The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

**Fields**

- Interface—Shows the interface names.
- ARP Inspection Enabled—Shows if ARP inspection is enabled, Yes or No.
- Flood Enabled—If ARP inspection is enabled, shows if the action is to flood unknown packets, Yes or No. If ARP inspection is disabled, this value is always No.
- Edit—Edits the ARP inspection parameters for the selected interface.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |

## Edit ARP Inspection Entry

The Edit ARP Inspection Entry dialog box lets you set ARP inspection settings.

**Fields**

- Enable ARP Inspection—Enables ARP inspection.
- Flood ARP Packets—Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet. If you do not check this check box, all non-matching packets are dropped.

**Note**

The default setting is to flood non-matching packets. To restrict ARP through the security appliance to only static entries, then set this command to **no-flood**.

The Management 0/0 interface or subinterface, if present, never floods packets even if this parameter is set to flood.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |

## ARP Static Table

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.



### Note

The transparent firewall uses dynamic ARP entries in the ARP table for traffic to and from the security appliance, such as management traffic.

The ARP Static Table panel lets you add static ARP entries that map a MAC address to an IP address for a given interface. Static ARP entries do not time out, and might help you solve a networking problem.

### Fields

- Interface—Shows the interface attached to the host network.
- IP Address—Shows the host IP address.
- MAC Address—Shows the host MAC address.
- Proxy ARP—Shows whether the security appliance performs proxy ARP for this address. If the security appliance receives an ARP request for the specified IP address, then it responds with the specified MAC address.
- Add—Adds a static ARP entry.
- Edit—Edits a static ARP entry.
- Delete—Deletes a static ARP entry.
- ARP Timeout—Sets the amount of time before the security appliance rebuilds the ARP table, between 60 to 4294967 seconds. The default is 14400 seconds. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently. Although this parameter appears on the ARP Static Table panel, the timeout applies to the *dynamic* ARP table.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit ARP Static Configuration

The Add/Edit ARP Static Configuration dialog box lets you add or edit a static ARP entry.

### Fields

- Interface—Sets the interface attached to the host network.
- IP Address—Sets the host IP address.
- MAC Address—Sets the host MAC address; for example, 00e0.1e4e.3d8b.
- Proxy ARP—Enables the security appliance to perform proxy ARP for this address. If the security appliance receives an ARP request for the specified IP address, then it responds with the specified MAC address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Customizing the MAC Address Table

This section describes the MAC address table, and includes the following topics:

- [MAC Address Table, page 30-4](#)
- [Add/Edit MAC Address Entry, page 30-6](#)
- [MAC Learning, page 30-6](#)

## MAC Address Table

The MAC Address Table pane lets you add static MAC Address entries. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the security appliance



drops the traffic and generates a system message. When you add a static ARP entry (see the [“ARP Static Table” section on page 30-3](#)), a static MAC address entry is automatically added to the MAC address table.

The security appliance learns and builds a MAC address table in a similar way as a normal bridge or switch: when a device sends a packet through the security appliance, the security appliance adds the MAC address to its table. The table associates the MAC address with the source interface so that the security appliance knows to send any packets addressed to the device out the correct interface.

The ASA 5505 adaptive security appliance includes a built-in switch; the switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN. This section discusses the bridge MAC address table, which maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

Because the security appliance is a firewall, if the destination MAC address of a packet is not in the table, the security appliance does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly connected devices or for remote devices:

- Packets for directly connected devices—The security appliance generates an ARP request for the destination IP address, so that the security appliance can learn which interface receives the ARP response.
- Packets for remote devices—The security appliance generates a ping to the destination IP address so that the security appliance can learn which interface receives the ping reply.

The original packet is dropped.

#### Fields

- Interface—Shows the interface associated with the MAC address.
- MAC Address—Shows the MAC address.
- Add—Adds a static MAC address entry.
- Edit—Edits a static MAC address entry.
- Delete—Deletes a static MAC address entry.
- Dynamic Entry Timeout—Sets the time a MAC address entry stays in the MAC address table before timing out, between 5 and 720 minutes (12 hours). 5 minutes is the default.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |

## Add/Edit MAC Address Entry

The Add/Edit MAC Address Entry dialog box lets you add or edit a static MAC address entry. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the security appliance drops the traffic and generates a system message.

### Fields

- Interface Name—Sets the interface associated with the MAC address.
- MAC Address—Sets the MAC address.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |

## MAC Learning

The MAC Learning pane lets you disable MAC address learning on an interface. By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired; however, unless you statically add MAC addresses to the table, no traffic can pass through the security appliance.

### Fields

- Interface—Shows the interface name.
- MAC Learning Enabled—Shows if MAC learning is enabled, Yes or No.
- Enable—Enables MAC learning to the selected interface.
- Disable—Disables MAC learning to the selected interface.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| —             | •           | •                | •        | —      |



## **PART 4**

### **Configuring VPN**





# CHAPTER 31

## SSL VPN Wizard

### SSL VPN Feature

Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. Users have no direct access to resources on the internal network.

The Cisco AnyConnect VPN client provides secure SSL connections to the security appliance 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 SSL VPN connections. The security appliance downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates. In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

#### Fields

- **Clientless SSL VPN Access**—Enables clientless, browser-based connections for specific, supported internal resources through a portal page.
- **Cisco SSL VPN Client (AnyConnect VPN Client)**—Enables SSL VPN client connections for full network access. Enables the security appliance to download the AnyConnect client to remote users.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## SSL VPN Interface

Provide a Connection name (previously called *tunnel group*), enable an interface for SSL VPN connections, and provide digital certificate information in this window.

### Fields

- Connection Name—Provide a connection name for this group of connection-oriented attributes.
- SSL VPN Interface—Specify the interface to allow SSL VPN connections.
- Digital Certificate—Specify a certificate, if any, that the security appliance sends to the remote PC.
  - Certificate—Specify the name of the certificate.
- Connection Group Settings—You can enable the security appliance to display a group alias for this connection on the login page.
  - Connection Group Alias—Specify an alias name for the connection.
  - Display Group Alias list at the login page—Enable to display the group alias.
- Information—Displays information remote users need for establishing SSL VPN connections and ASDM connections.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## User Authentication

Specify authentication information on this screen.

### Fields

- Authenticate using a AAA server group—Enable to let the security appliance contact a remote AAA server group to authenticate the user.
- AAA Server Group Name—Select a AAA server group from the list of pre-configured groups, or click **New** to create a new group.
- Authenticate using the local user database—Add new users to the local database stored on the security appliance.
  - 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.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Group Policy

Group policies configure common attributes for groups of users. Create a new group policy or select an existing one to modify.

**Fields**

- Create new group policy—Enable to create a new group policy. Provide a name for the new policy.
- Modify existing group policy—Select an existing group policy to modify.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Bookmark List

Bookmark lists appear on the portal page for Clientless, browser-based connections. SSL VPN client users do not see these bookmarks. Create a new bookmark list on this window.

**Fields**

- Bookmark List—Select an existing list or click **Manage** to create a new list, or import or export bookmark lists.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## IP Address Pools and Client Image

Provide a range of IP addresses to remote SSL VPN users and identify SSL VPN client images to the security appliance in this window.

### Fields

- IP Address Pool—SSL VPN clients receive new IP addresses when they connect to the security appliance. Clientless connections do not require new IP addresses. Address Pools define a range of addresses that remote clients can receive.
- IP Address Pool—Select an existing IP Address Pool, or click **New** to create a new pool.
- AnyConnect VPN Client Image Location—Identify to the security appliance files in flash memory that are SSL VPN client images. Click Browse to locate images on your local PC.
  - Location—Provide the path and filename of a valid SSL VPN client image located in flash memory.
  - Download Latest AnyConnect VPN Client form CCO—Click this link to go to the Software Download page for the latest client image.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Summary

Provides a summary of your selections from the previous wizard windows.

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |





## CHAPTER 32

# VPN

---

The security appliance 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 security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance 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 security appliance performs the following VPN functions:

- Establishes tunnels.
- Negotiates tunnel parameters.
- Enforces VPN policies.
- Authenticates users.
- Authorizes users for specific levels of use and access.
- Performs accounting functions.
- Assigns user addresses.
- Encrypts and decrypts data.
- Manages security keys.
- Manages data transfer across the tunnel.
- Manages data transfer inbound and outbound as a tunnel endpoint or router.

The security appliance invokes various standard protocols to accomplish these functions.

## VPN Wizard

The VPN wizard lets you configure basic LAN-to-LAN and remote access VPN connections. Use ASDM to edit and configure advanced features.

**Note**

The VPN wizard lets you assign either preshared keys or digital certificates for authentication. However, to use certificates, you must enroll with a certification authority and configure a trustpoint prior to using the wizard. Use the ASDM Device Administration > Certificate panels and online Help to accomplish these tasks.

**VPN Overview**

The security appliance 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 security appliance uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The security appliance 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 security appliance performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

## VPN Tunnel Type

Use the VPN Tunnel Type panel to select the type of VPN tunnel to define, remote access or LAN-to-LAN, and to identify the interface that connects to the remote IPSec peer.

**Fields**

- **Site-to-Site**—Click to create a LAN-to-LAN VPN configuration. Use between two IPSec security gateways, which can include security appliances, VPN concentrators, or other devices that support site-to-site IPSec connectivity. When you select this option, the VPN wizard displays a series of panels that let you to enter the attributes a site-to-site VPN requires.
- **Remote Access**—Click to create a configuration that achieves secure remote access for VPN clients, such as mobile users. This option lets remote users securely access centralized network resources. When you select this option, the VPN wizard displays a series of panels that let you enter the attributes a remote access VPN requires.
- **VPN Tunnel Interface**—Select the interface that establishes a secure tunnel with the remote IPSec peer. If the security appliance 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.

- Enable inbound IPSec sessions to bypass interface access lists—Enable IPSec authenticated inbound sessions to always be permitted through the security appliance (that is, without a check of 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Remote Site Peer

Use the Remote Site Peer panel for the following tasks:

1. Providing the IP address of the remote IPSec peer that terminates this VPN tunnel.
2. Creating the for the remote peer.
3. Selecting and configuring an authentication method.

### Fields

- Peer IP Address—Type the IP address of the remote IPSec peer that terminates the VPN tunnel. The peer might be another security appliance, a VPN concentrator, or any other gateway device that supports IPSec.
- 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 security appliance and the remote IPSec peer.

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.

- Pre-shared Key—Type the preshared key. Maximum 127 characters.
- Certificate—Click to use certificates for authentication between the local security appliance 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 security appliance.

Digital certificates are an efficient way to manage the security keys used to establish an IPSec tunnel. 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 owner's 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—Select the algorithm for signing digital certificates, either rsa-sig for RSA or dsa-sig for DSA.
- Trustpoint Name—Select the name that identifies the certificate the security appliance sends to the remote peer. This list displays trustpoints with a certificate of the type previously selected in the certificate signing algorithm list.
- Challenge/response authentication (CRACK)—Provides strong mutual authentication when the client authenticates using a popular method such as RADIUS and the server uses public key authentication. The security appliance supports CRACK as an IKE option in order to authenticate the Nokia VPN Client on Nokia 92xx Communicator Series devices.
- Name—Type a name to create the record that contains tunnel connection policies for this IPSec connection. A can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes. A that you configure with this VPN wizard specifies an authentication method, and uses the security appliance Default Group Policy.

By default, ASDM populates this box with the value of the Peer IP address. You can change this name. Maximum 64 characters.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## 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 panel to set the terms of the Phase 1 IKE negotiations, which include the following:

- An encryption method to protect the data and ensure privacy.
- An authentication method to ensure the identity of the peers.
- A Diffie-Hellman group to establish the strength of the of the encryption-key-determination algorithm. The security appliance uses this algorithm to derive the encryption and hash keys.

**Fields**

- **Encryption**—Select the symmetric encryption algorithm the security appliance uses to establish the Phase 1 SA that protects Phase 2 negotiations. The security appliance 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**—Select 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 security appliance prevents this attack.
- **DH 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 2 (1024-bit Diffie-Hellman), requires less CPU time to execute but is less secure than Group 5 (1536-bit). Group 7 is for use with the Movian VPN client, but works with any peer that supports Group 7 (ECC).

**Note**

The default value for the VPN 3000 Series Concentrator is MD5. A connection between the security appliance and the VPN Concentrator requires that the authentication method for Phase I and II IKE negotiations be the same on both sides of the connection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## IPSec Encryption and Authentication

Use this IPSec Encryption and Authentication panel to select the encryption and authentication methods to use for Phase 2 IKE negotiations, which create the secure VPN tunnel. These values must be exactly the same for both peers.

**Fields**

- **Encryption**—Select the symmetric encryption algorithm the security appliance uses to establish the VPN tunnel. The security appliance uses encryption to protect the data that travels across the tunnel and ensure privacy. Valid encryption methods include the following:

**Encryption**

| Method  | Explanation                                          |
|---------|------------------------------------------------------|
| DES     | Data Encryption Standard. Uses a 56-bit key.         |
| 3DES    | Triple DES. Encrypts 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**—Select 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 security appliance prevents this attack.

**Note**

The default value for the VPN 3000 Series Concentrator is MD5. A connection between the security appliance and the VPN Concentrator requires that the authentication method for Phase I and Phase II IKE negotiations be the same on both sides of the connection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Hosts and Networks

Use the Hosts and Networks panel to identify local and remote hosts and networks that can use this LAN-to-LAN IPSec tunnel to send and receive data.

For IPSec to succeed, both peers in the LAN-to-LAN connection must have compatible entries for hosts and networks. The hosts and networks you configure as Local Hosts and Networks in this panel must be configured as Remote Hosts and Networks on the device at the remote site for the LAN-to-LAN connection. The local security appliance and the remote device must have at least one transform set in common for this LAN-to-LAN connection.



**Fields**

- Action—Decide whether or not to protect data travelling between the local and remote network.
- Local networks—Select the local hosts and networks.
- Remote networks—Select the remote hosts and networks.
- Exempt ASA side host/network from address translation—Allows traffic to pass through the security appliance without address translation.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Summary

The Summary panel displays all of the attributes of this VPN LAN-to-LAN connection as configured.

**Fields**

**Back**—To make changes, click **Back** until you reach the appropriate panel.

**Finish**—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.

**Cancel**—To remove the configuration, click **Cancel**.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Remote Access Client

Use the Remote Access Client panel to identify the type of remote access users this connection serves.

**Fields**

- Cisco VPN Client Release 3.x or higher, or other Easy VPN Remote product—Click for IPSec connections, including compatible software and hardware clients other than those named here.

- Microsoft Windows client using L2TP over IPSec—Click to enable connections from Microsoft Windows and Microsoft Windows Mobile clients over a public IP network. L2TP uses PPP over UDP (port 1701) to tunnel the data. Enable one or more of the following PPP authentication protocols:
  - PAP—Passes 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 the 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—Enables EAP which permits the security appliance to proxy the PPP authentication process to an external RADIUS authentication server.
- Client will send name as username@tunnelgroup—Check to enable the security appliance to associate different users that are establishing L2TP over IPSec connections with different s. Since each has its own AAA server group and IP address pools, users can be authenticated through methods specific to their .

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## VPN Client Authentication Method and Name

Use the VPN Client Authentication Method and Name panel to configure an authentication method and create a .

### Fields

- 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 security appliance and the remote IPSec peer.
 

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.
  - Pre-shared Key—Type the preshared key.

- **Certificate**—Click to use certificates for authentication between the local security appliance 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 security appliance.

Digital certificates are an efficient way to manage the security keys used to establish an IPSec tunnel. 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 owner's 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.

- **Trustpoint Name**—Select the name that identifies the certificate the security appliance sends to the remote peer.
- **Certificate Signing Algorithm**—Select the algorithm for signing digital certificates, either rsa-sig for RSA or dsa-sig for DSA.
- **Challenge/response authentication (CRACK)**—Provides strong mutual authentication when the client authenticates using a popular method such as RADIUS and the server uses public key authentication. The security appliance supports CRACK as an IKE option in order to authenticate the Nokia VPN Client on Nokia 92xx Communicator Series devices.
- **Name**—Type a name to create the record that contains tunnel connection policies for this IPSec connection. A can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes. A that you configure with this VPN wizard specifies an authentication method, and uses the security appliance Default Group Policy.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Client Authentication

Use the Client Authentication panel to select the method by which the security appliance authenticates remote users.

### Fields

Select one of the following options:

- **Authenticate using the local user database**—Click to use authentication internal to the security appliance. Use this method for environments with a small, stable number of users. The next panel lets you create accounts on the security appliance for individual users.

- Authenticate using an AAA server group—Click to use an external server group for remote user authentication.
- AAA Server Group—Select a AAA server group configured previously.
- New ...—Click to configure a new AAA server group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## New Authentication Server Group

User the New Authentication Server Group panel to define one or more new AAA servers.

### Fields

To configure a new AAA server group that contains just one server, provide the following information:

- Server Group Name—Type a name for the server group. You associate this name with users whom you want to authenticate using this server.
- Authentication Protocol—Select the authentication protocol the server uses. Options include TACACS+, RADIUS, SDI, NT, and Kerberos.
- Server IP Address—Type the IP address for the AAA server.
- Interface—Select the security appliance interface on which the AAA server resides.
- Server Secret Key—Type a case-sensitive, alphanumeric keyword of up to 127 characters. The server and security appliance use the key to encrypt data that travels between them. The key must be the same on both the security appliance and server. You can use special characters, but not spaces.
- Confirm Server Secret Key—Type the secret key again.

To add more servers to this new group, or to change other AAA server settings, go to Configuration > Features > Properties > AAA.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## User Accounts

Use the User Accounts panel to add new users to the security appliance internal user database for authentication purposes.

### Fields

Provide the following information:

- User to Be Added—Use the fields in this section to add a user.
  - Username—Enter the username.
  - Password—(Optional) Enter a password.
  - Confirm Password—(Optional) Reenter the password.
- Add — Click to add a user to the database after you have entered the username and optional password.
- Username—Displays the names of all users in the database.
- Delete—To remove a user from the database, highlight the appropriate username and click **Delete**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Address Pool

Use the Address Pool panel to configure a pool of local IP addresses that the security appliance assigns to remote VPN clients.

### Fields

- Name—Displays the name of the tunnel group to which the address pool applies. You set this name in the VPN Client Name and Authentication Method panel.
- 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) Select the subnet mask for these IP addresses

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Attributes Pushed to Client

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

### Fields

Provide information for remote access clients to use.

- —Displays the name of the to which the address pool applies. You set this name in the VPN Client Name and Authentication Method panel.
- 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. Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Address Translation Exemption

Use the Address Translation Exemption (Optional) panel to identify local hosts/networks which do not require address translation. By default, the security appliance 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 panel. If you have even one entry, all other hosts and networks are subject to NAT.

### Fields

- **Host/Network to Be Added**—Complete these fields to exempt a particular host or network from NAT.
  - **Interface**—Select the name of the interface that connects to the hosts or networks you have selected.
  - **IP address**—Select the IP address of the host or network. Either type the IP address or click the adjacent ... button to view a diagram of the network and select a host or network.
- **Add**—Click to add the host or network the Selected Hosts/Networks list after you have completed the applicable fields.
- **Selected Hosts/Networks**—Displays the hosts and networks that are exempt from NAT. If you want all hosts and networks to be exempt from NAT, leave this list empty.
- **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 security appliance 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 security appliance. All other traffic travels unencrypted directly to the Internet without involving the security appliance.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |







## CHAPTER 33

# Configuring Certificates

---

Digital certificates provide digital identification for authentication. A digital certificate contains information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs issue digital certificates in the context of a PKI, which uses public-key/private-key encryption to ensure security. CAs are trusted authorities that “sign” certificates to verify their authenticity, thus guaranteeing the identity of the device or user.

For authentication using digital certificates, there must be at least one identity certificate and its issuing CA certificate on a security appliance, which allows for multiple identities, roots and certificate hierarchies. There a number of different types of digital certificates listed below:

- A *CA certificate* is one used to sign other certificates. A CA certificate that is self-signed is called a *root certificate*; one issued by another CA certificate is called a *subordinate certificate*. See [CA Certificate Authentication](#).
- CAs also issue *identity certificates*, which are the certificates for specific systems or hosts. See [Identity Certificates Authentication](#).
- *Code-signer certificates* are special certificates used to create digital signatures to sign code, with the signed code itself revealing the certificate origin. See [Code-Signer Certificates](#)
- The Local Certificate Authority (CA) integrates an independent certificate authority functionality on the security appliance, deploys certificates, and provides secure revocation checking of issued certificates. The Local CA provides a secure configurable inhouse authority for certificate authentication with user enrollment by browser web page login. See [Local Certificate Authority](#), [Manage User Certificates](#), and [Manage User Database](#).

## CA Certificate Authentication

The CA Certificates panel allows you to authenticate self-signed or subordinate CA certificates and to install them on the security appliance. You can create a new certificate configuration or you can edit an existing one.

If the certificate you select is configured for manual enrollment, you should obtain the CA certificate manually and import it here. If the certificate you select is configured for automatic enrollment, the security appliance uses the SCEP protocol to contact the CA, and then automatically obtains and installs the certificate.

## CA Certificates Fields

Configuration > Remote Access VPN > Certificate Management > CA Certificates

| Issued To            | Issued By                      | Expiry Date              | Usage           |
|----------------------|--------------------------------|--------------------------|-----------------|
| Cisco Systems Sub2   | [cn=Cisco Systems Sub1]        | 11:01:07 EST Mar 15 2007 | Signature       |
| asa1.frga.cisco.com  | [cn=asa1.frga.cisco.com]       | 02:36:44 EST Feb 14 2010 | Signature       |
| ms-root-ca-5-2004    | [cn=ms-root-ca-5-2004, ou=F... | 08:34:52 EST May 20 2024 | General Purpose |
| Cisco Systems Sub1   | [cn=Cisco Systems]             | 11:01:07 EST Mar 15 2007 | Signature       |
| wb5520-FO.wbrown.com | [cn=wb5520-FO.wbrown.com]      | 10:55:31 EST Feb 5 2010  | Signature       |
| Cisco Systems        | [cn=Cisco Systems]             | 18:06:36 EST Mar 13 2011 | Signature       |

Buttons: Add, Edit, Show Details, Request CRL, Delete

Buttons: Apply, Reset

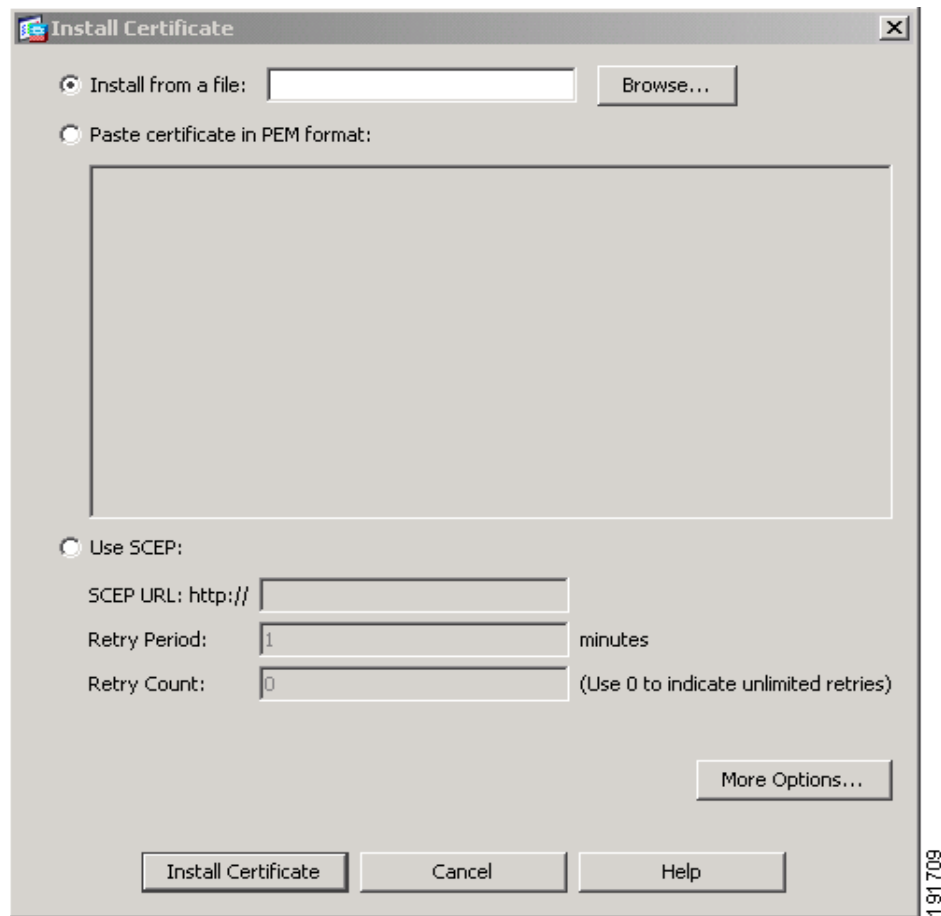
- **Certificates**—Displays a list of the certificates available identified by issued to and by, the date the certificate expires, and the certificate's usage or purpose. You can click a certificate in the list and edit its configuration, or you can add a new certificate to the displayed list.
- **Add Button**—Add a new certificate configuration to the list. See [Add/Install a CA Certificate](#).
- **Edit Button**—Modify an existing certificate configuration. See [Edit CA Certificate Configuration](#).
- **Show Details Button**—Display the details and issuer information for the selected certificate. See [Show CA Certificate Details](#).
- **Request CRL Button**—Access the Certificate Revocation List (CRL) for an existing CA certificate. See [Request CRL](#).
- **Delete Button**—Remove the configuration of an existing CA certificate. See [Delete a CA Certificate](#).
- **Apply Button**—Save the new or modified CA certificate configuration.
- **Reset Button**—Remove any edits and return the display to the original contents.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

## Add/Install a CA Certificate



The CA Certificate panel lets you add a new certificate configuration from an existing file, by manually pasting a certificate, or by automatic enrollment. Click the appropriate option to activate one of the following:

- **Install from a File:**—To add a certificate configuration from an existing file, enter the path and file name, then click **Install Certificate**. You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the Load CA certificate file dialog box that lets you navigate to the file containing the certificate.
- **Paste certificate in PEM format:**—For manual enrollment, copy and paste the PEM format certificate (base64 or hexadecimal format) into the panel, then click **Install Certificate**.
- **Use SCEP:**—For automatic enrollment, the security appliance contacts the CA using Simple Certificate Enrollment Protocol (SCEP) protocol, obtains the certificates, and installs them on the device. (SCEP). SCEP is a secure messaging protocol that requires minimal user intervention. SCEP lets you to enroll and install certificates using only the VPN Concentrator Manager. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet.

SCEP automatic enrollment requires completion of the following fields:

- **SCEP URL: HTTP://** Enter the path and file name of the certificate to be automatically installed.

- **Retry Period:** Specify the maximum number of minutes to retry installing a certificate. The default is one minute.
- **Retry Count:** Specify the number of retries for installing a certificate. The default is 0, which indicates unlimited retries within the retry period.

**More Options...** —For additional options for new certificates, click the **More Options...** button to display configuration options for new and existing certificates. See [Configuration Options for CA Certificates](#).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

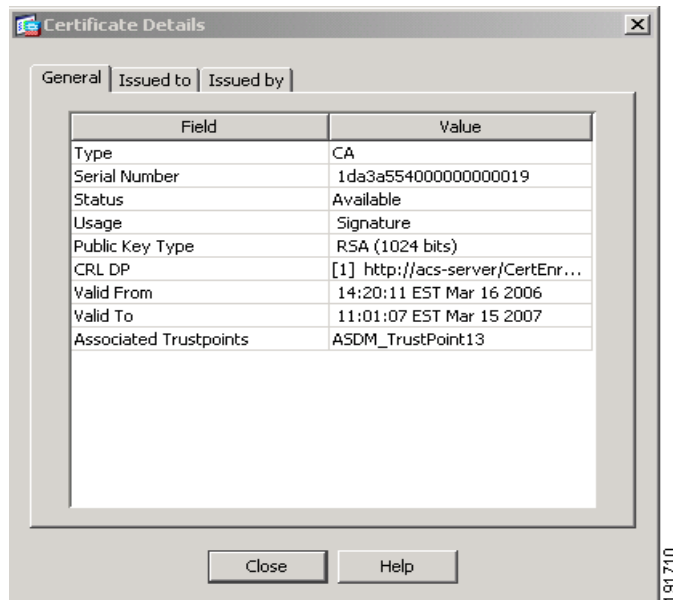
### Edit CA Certificate Configuration

To modify the characteristics of an existing certificate, select the certificate and click the **Edit** button to display a number of tab-selectable displays that address CA certificate configuration specifics. For details, see [Configuration Options for CA Certificates](#).

### Show CA Certificate Details

The **Show Details** button displays the Certificate Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.
- **Issued to**—Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.



191710

## Request CRL

The **Request CRL** button updates the current version of the Certificate Revocation List (CRL). CRL update provides the current status of certificate users. If the request fails, an error message displays.

The CRL is generated and regenerated automatically until it expires; the **Request CRL** button forces an immediate CRL file update and regeneration.

## Delete a CA Certificate

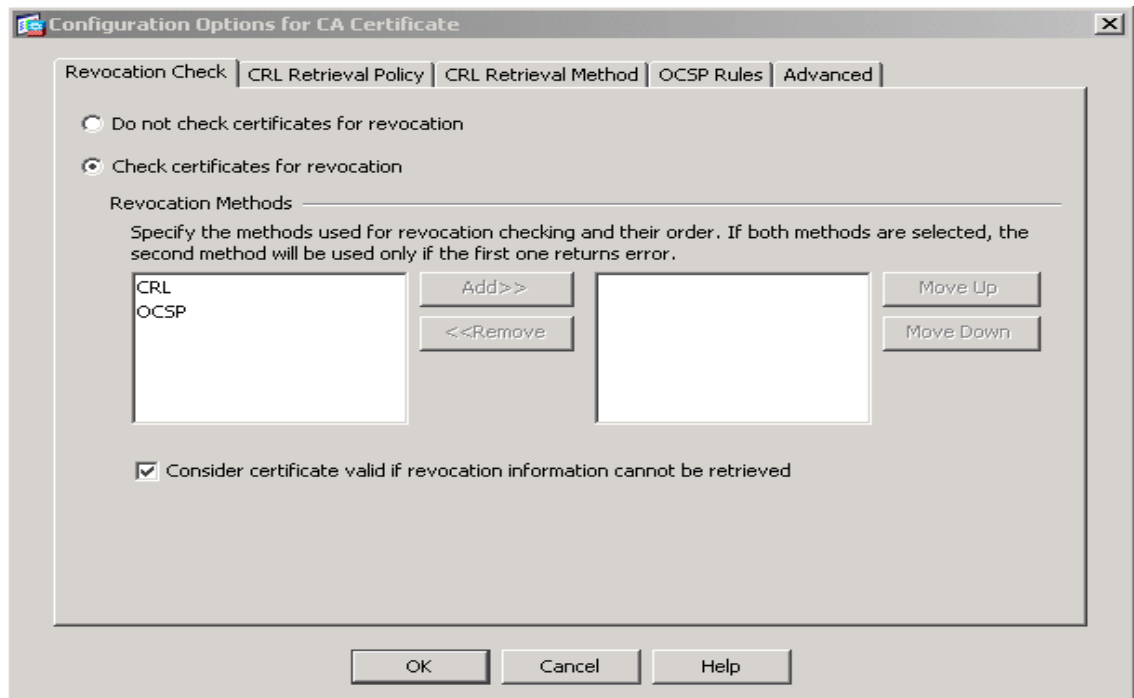
The **Delete** button immediately removes the selected CA Certificate configuration from the security appliance. Once you delete a certificate configuration, it cannot be restored; to recreate the deleted certificate, you must use the **Add** button to reenter the certificate configuration information from the beginning.



**Note** Once you delete a certificate configuration, it cannot be restored.

## Configuration Options for CA Certificates

Additional configuration options are available, whether you are adding a new CA certificate with the **Add** button or modifying an existing CA certificate with the **Edit** button.



The following panels are the tab-selectable displays that address CA certificate configuration specifics. Each tabbed display is summarized in the following list:

**Revocation Check**—The Revocation Check panel lets you choose or reject revocation checking, specify a method of revocation checking (CRL or OCSP) and allows you to ignore revocation-checking errors when validating a certificate. For details of the Revocation Check panel, see [Revocation Check Configuration](#).

**CRL Retrieval Policy**—The CRL Retrieval Policy panel allows you to configure use of the CRL distribution point and/or static CRL URLs, with capabilities to add, edit, and delete status CRL URLs. For details, see [CRL Retrieval Policy Configuration](#).

**CRL Retrieval Method**—The CRL Retrieval Method panel allows you to choose Lightweight Directory Access Protocol (LDAP), HTTP, or Simple Certificate Enrollment Protocol (SCEP) as the method to be used for CRL retrieval. For the LDAP method, you can configure the LDAP parameters and security. See [CRL Retrieval Method Configuration](#).

**OCSP Rules**—Online Certificate Status Protocol (OCSP) is used for obtaining revocation status of an X.509 digital certificate and is an alternative to certificate revocation lists (CRL). For details, see [OCSP Rules Configuration](#). Refer to [OCSP Rules Configuration](#).

**Advanced**—The Advanced panel allows you to set up CRL update parameters, OCSP parameters, and certificate acceptance and validation parameters. See [Advanced Configuration Options](#).

#### Revocation Check Configuration

With the **Revocation Check** Edit Option panel, you can specify degrees of user certificate revocation checking as follows:

No Revocation Checking - Click the **Do not check certificates for revocation** button to disable revocation checking of certificates.

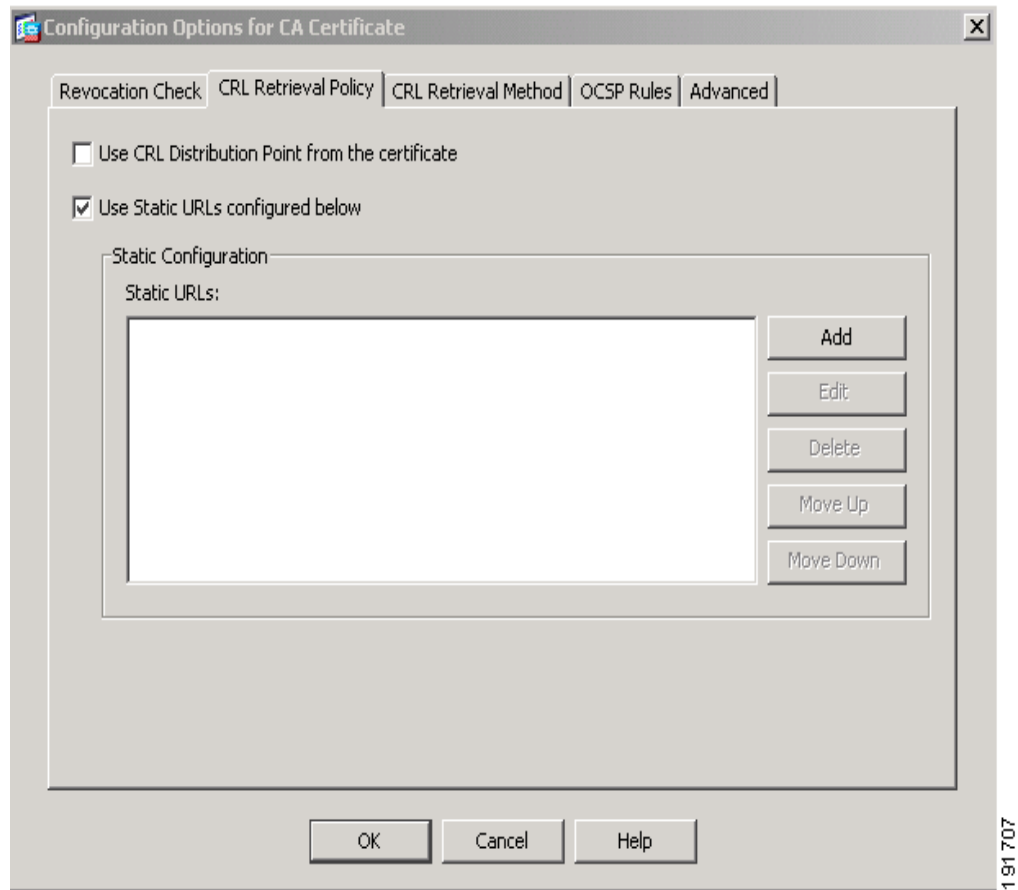
Revocation Checking Method(s) - Click the **Check certificates for revocation** to select one or more revocation checking methods. Available methods display on the left; use the **Add** button to move a method to the right.

The methods you select are implemented in the order in which you add them. If a method detects an error, subsequent revocation checking methods activate.

**Revocation Checking Override** - Click the **Consider certificate valid if revocation checking returns errors** button to ignore revocation-checking errors.

### CRL Retrieval Policy Configuration

With the CRL Retrieval Policy panel, you specify either the CRL Distribution Point, or a static go-to location for the CRL revocation checking.

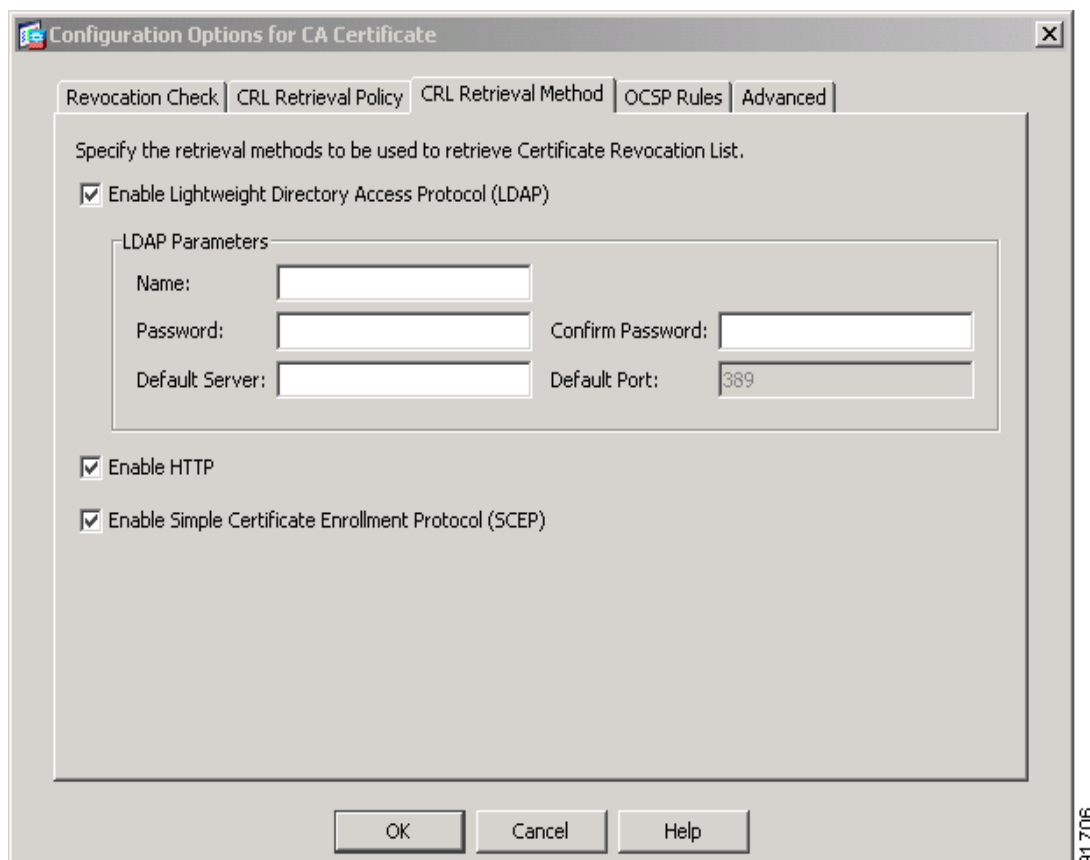


- **Certificate CRL Distribution Point** - Click the **Use CRL Distribution Point from the certificate** button to direct revocation checking to the CRL DP included on the certificate being checked.
- **Static URL** - Click the **Use Static URLs configured below** button to list specific URLs to be used for CRL Retrieval. The URLs you select are implemented in the order in which you add them. If a specified URL errors, subsequent URLs are accessed in order.

://—Type the location that distributes the CRLs.

### CRL Retrieval Method Configuration

The CRL Retrieval Method panel lets you select the method to be used for CRL retrieval.

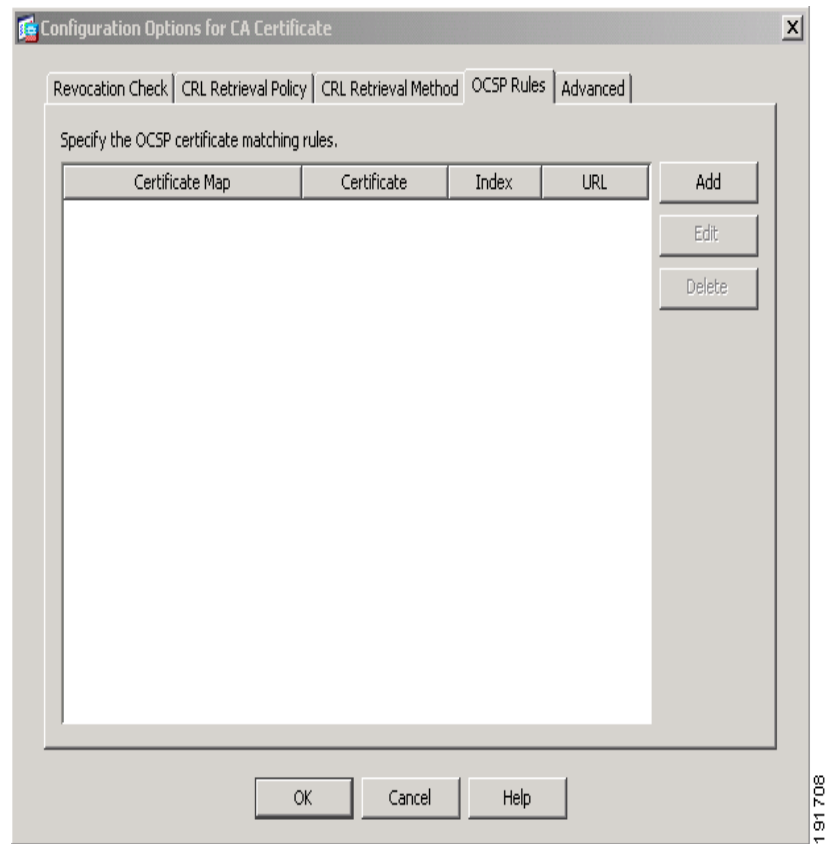


- Click the **Enable Lightweight Directory Access Protocol (LDAP)** button to specify LDAP CRL retrieval. With LDAP, CRL retrieval starts an LDAP session by connecting to a named LDAP server, accessed by password. The connection is on TCP port 389 by default. Enter the specific LDAP parameters required:
  - Name:
  - Password:
  - Confirm Password:
  - Default Server: (server name)
  - Default Port: 389 (default)
- HTTP - Click the **Enable HTTP button** to select HTTP CRL retrieval
- SCEP - Click the **Enable Simple Certificate Enrollment Protocol (SCEP)** to select SCEP for CRL retrieval.

### OCSP Rules Configuration

The Online Certificate Status Protocol (OCSP) panel lets you configure OCSP rules for obtaining revocation status of an X.509 digital certificate.



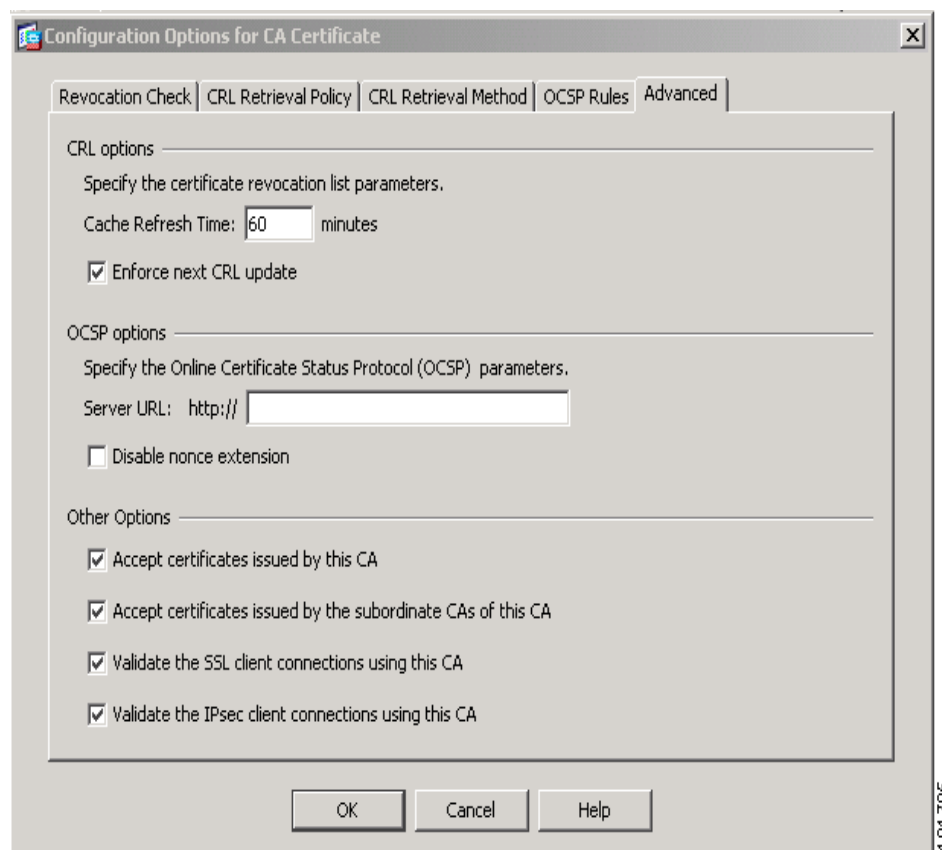


### OCSP Rules Fields

- **Certificate Map**—Displays the name of the certificate map to match to this OCSP rule. Certificate maps match user permissions to specific fields in a certificate. You must configure the certificate map before you configure OCSP rules.
- **Certificate**—Displays the name of the CA the security appliance uses to validate responder certificates.
- **Index**—Displays the priority number for the rule. The security appliance examines OCSP rules in priority order, and applies the first one that matches.
- **URL**—Specifies the URL for the OCSP server for this certificate.
- **Add**—Click to add a new OCSP rule.
- **Edit**—Click to edit an existing OCSP rule.
- **Delete**—Click to delete an OCSP rule.

### Advanced Configuration Options

The **Advanced** tab lets you specify CRL and OCSP options. When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, due to security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the security appliance to check that the CA has not revoked the certificate being verified.



The security appliance supports two methods of checking revocation status: CRL and OCSP.

#### Fields

- **CRL Options**

- **Cache Refresh Time**—Specify the number of minutes between cache refreshes. The default number of minutes is 60. The range is 1-1440.

To avoid having to retrieve the same CRL from a CA repeatedly, The security appliance can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the security appliance removes the least recently used CRL until more space becomes available.

- **Enforce next CRL update**—Require valid CRLs to have a Next Update value that has not expired. Clearing the box allows valid CRLs with no Next Update value or a Next Update value that has expired.

- **OCSP Options**

- **Server URL:**—Enter the URL for the OCSP server. The security appliance uses OCSP servers in the following order:
  1. OCSP URL in a match certificate override rule
  2. OCSP URL configured in this OCSP Options attribute
  3. AIA field of remote user certificate

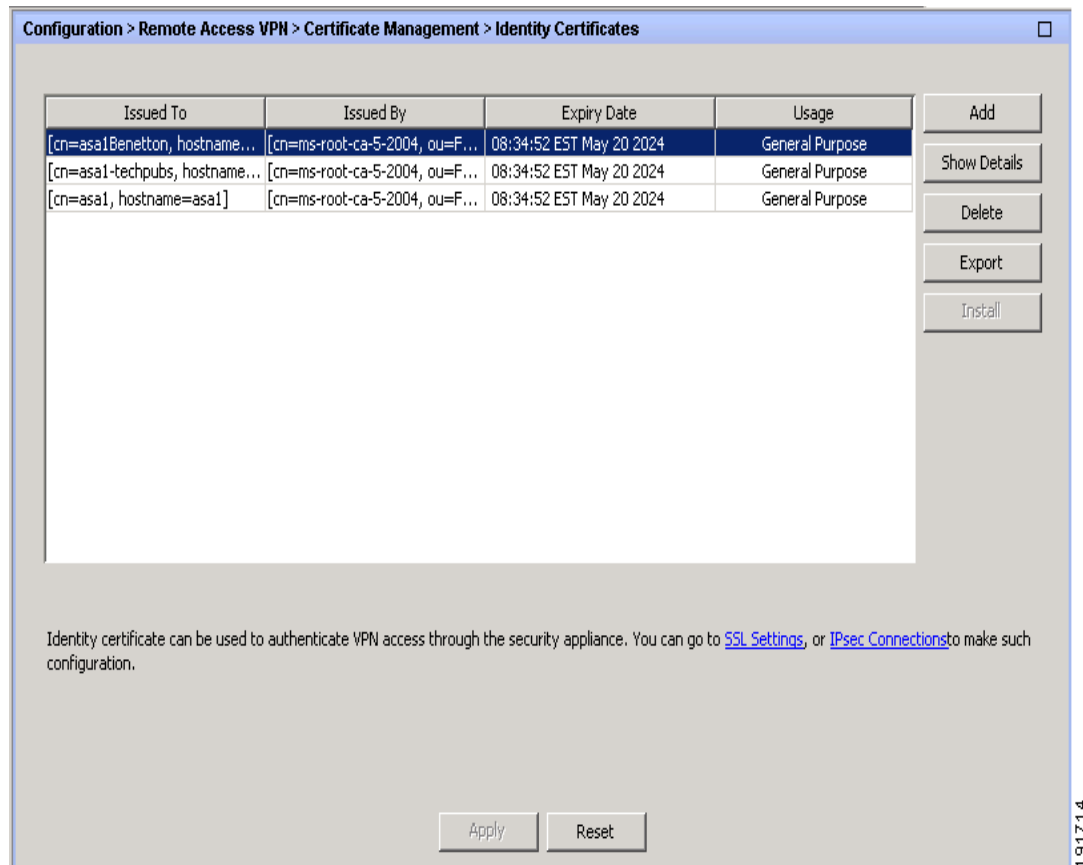
- **Disable nonce extension**—By default the OCSP request includes the nonce extension, which cryptographically binds requests with responses to avoid replay attacks. It works by matching the extension in the request to that in the response, ensuring that they are the same. Disable the nonce extension if the OCSP server you are using sends pre-generated responses that do not contain this matching nonce extension.
- **Validation Policy**
  - **Specify the type of client connections that can be validated by this CA**—Click SSL or IPSec to restrict the type of remote session this CA can be used to validate, or click SSL and IPSec to let the CA validate both types of sessions.
- **Other Options**
  - **Accept certificates issued by this CA**—Specify whether or not the security appliance should accept certificates from **CA Name**.
  - **Accept certificates issued by the subordinate CAs of this CA**

## Identity Certificates Authentication

An Identity Certificate can be used to authenticate VPN access through the security appliance. Click the *SSL Settings* or the *IPsec Connections* links on the Identity Certificates panel for additional configuration information.

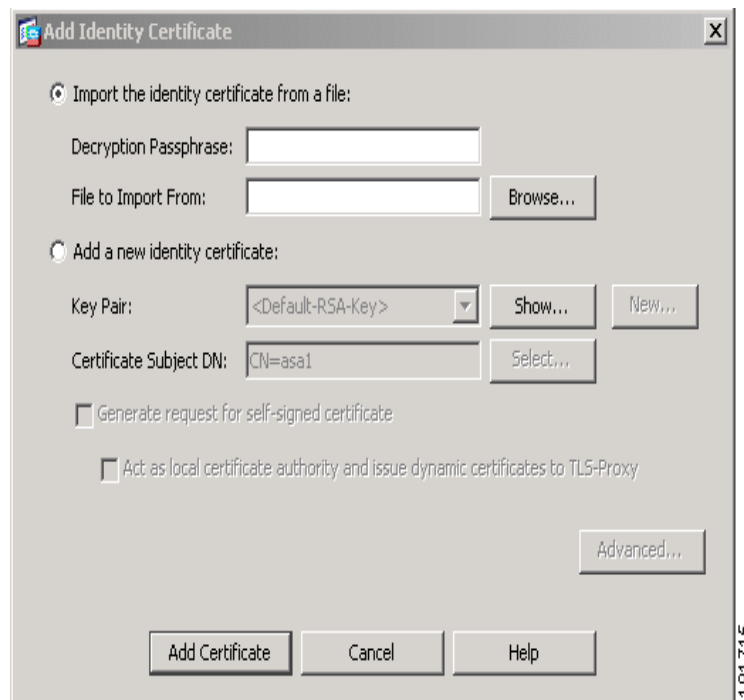
The Identity Certificates Authentication panel allows you to:

- Add an Identity Certificate. See [Add/Install an Identity Certificate](#).
- Display details of an Identity Certificate. See [Show Identity Certificate Details](#).
- Delete an existing Identity Certificate. See [Delete an Identity Certificate](#).
- Export an existing Identity Certificate. See [Export an Identity Certificate](#).
- Install an Identity Certificate. See [Installing Identity Certificates](#).
- Enroll for a certificate with Entrust. See [Generate](#)



### Add/Install an Identity Certificate

The Identity Certificate panel lets you import an existing identity certificate from a file or add a new certificate configuration from an existing file.



Click the appropriate option to activate one of the following:

#### Add Identity Certificate Fields

Assign values to the fields in the **Add Identity Certificate** dialog box as follows:

- To import an identity certificate from an existing file, select **Import the identity certificate from a file** and enter the following information:
  - Decryption Pass Phrase—Specify the passphrase used to decrypt the PKCS12 file.
  - File to Import From—You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the Load Identity Certificate file dialog box that lets you navigate to the file containing the certificate.
- To add a new identity certificate requires the following information:—
  - Key Pair—RSA key pairs are required to enroll for identity certificates. The security appliance supports multiple key pairs.
  - Key Pair name (in Key Pair > Show window)— Specifies name of the key pair whose public key is to be certified.
  - Generation time (in Key Pair > Show window)—Displays time of day and the date when the key pair is generated.
  - Usage (in Key Pair > Show window)— Displays how an RSA key pair is to be used. There are two types of usage for RSA keys: *general purpose* (the default) and *special*. When you select *Special*, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
  - Modulus Size (bits) (in Key Pair > Show window)— Displays the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
  - Key Data: (in Key Pair > Show window)—Indicates the window that contains the specific key data

- Name (in Key Pair > New window)—Selects a default key pair name, such as <Default-RSA-Key>, or you can enter a new key pair name.
- Size (in Key Pair > New window)—Specifies the default key pair size: 512, 788, 1024 (the default) or 2048.
- Usage (in Key Pair > New window)— Specifies the key pair usage as *general purpose* or *special*.
- The **Advanced** button on the **Add Identity Certificate** pane lets you establish the following certificate parameters, enrollment mode, and an optional revocation password for the device-specific identity certificate:
  - **FQDN** (in Advanced > Certificate Parameters)—The Fully Qualified Domain Name (FQDN), an unambiguous domain name, specifies the position of the node in the DNS tree hierarchy.
  - **E-mail** (in Advanced > Certificate Parameters)— The e-mail address associated with the Identity Certificate.
  - **IP Address** (in Advanced > Certificate Parameters)—The security appliance address on the network in four-part dotted-decimal notation.
  - The check box **Include serial number of the device** allows you to add the security appliance serial number to the certificate parameters.
  - The Advanced > Enrollment Mode allows you to select either manual enrollment (**Request by manual enrollment**) or enrollment by CA (**Request from a CA**), which requires the following information:
    - **Enrollment URL (SCEP): HTTP://** Enter the path and file name of the certificate to be automatically installed.
    - **Retry Period:** Specify the maximum number of minutes to retry installing an Identity certificate. The default is one minute.
    - **Retry Count:** Specify the number of retries for installing an Identity certificate. The default is 0, which indicates unlimited retries within the retry period.
- In the **Add Identity Certificate** pane, enter the following Certificate Subject DN information:
  - **Certificate Subject DN**— Specify the certificate subject-name DN to form the DN in the Identity certificate, and click the **Select...** button to add DN attributes in the Certificate Subject DN pane.
  - **Attribute:** (in Certificate Subject DN > Select window)— Select one or more DN attributes from the pull-down menu. Selectable X.500 fields of attributes for the Certificate Subject DN are:

---

**Certificate Subject DN Attributes**


---

|                     |
|---------------------|
| CN = Common Name    |
| OU = Department     |
| O = Company Name    |
| C = Country         |
| ST = State/Province |
| L = Location        |
| EA = E-mail Address |

---

- **Value:** (in Certificate Subject DN > Select window)— Enter the value for each of the DN attributes that you select in the **Attribute** list. With a value assigned to an attribute, use the now-active **Add** button to add the attribute to the Attribute/Value field on the right. To remove attributes and their values, select the attribute and click the now-active **Delete** button.

Once you complete Identity Certificate configuration, click **Add Certificate** in the Add Identity Certificate pane. Then, be sure to click the **Apply** button in the **Identity Certificates** window to save the newly certificate configuration.

### Show Identity Certificate Details

The **Show Details** button displays the Certificate Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.
- **Issued to**— Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.

### Delete an Identity Certificate

The **Delete** button immediately removes the selected Identity Certificate configuration from the security appliance. Once you delete a certificate configuration, it cannot be restored; to recreate the deleted certificate, use the **Add** button to reenter the certificate configuration information from the beginning

**Note**

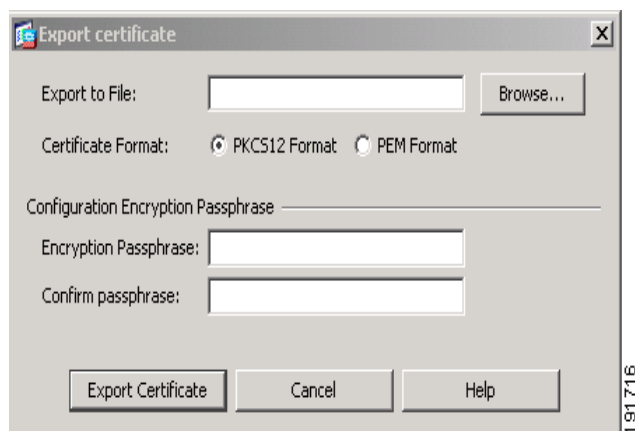
---

Once you delete a certificate configuration, it cannot be restored.

---

### Export an Identity Certificate

The **Export** panel lets you export a certificate configuration with all associated keys and certificates in PKCS12 format, which must be in base64 format. An entire configuration includes the entire chain (root CA certificate, identity certificate, key pair) but not enrollment settings (subject name, FQDN and so on). This feature is commonly used in a failover or load-balancing configuration to replicate certificates across a group of security appliances; for example, remote access clients calling in to a central organization that has several units to service the calls. These units must have equivalent certificate configurations. In this case, an administrator can export a certificate configuration and then import it across the group of security appliances.



### Export Identity Certificate Fields

- **Export to a file**—Specify the name of the PKCS12-format file to use in exporting the certificate configuration;
- **Certificate Format**—Click PKCS12 format, the public key cryptography standard, which can be base64 encoded or hexadecimal, or click PEM format.
  - **Browse**—Display the **Select a File** dialog box that lets you navigate to the file to which you want to export the certificate configuration.
- **Encryption Passphrase**—Specify the passphrase used to encrypt the PKCS12 file for export.
  - **Confirm Passphrase**—Verify the encryption passphrase.
- **Export Certificate**—Export the certificate configuration.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

## Generate Certificate Signing Request

This pane lets you generate a certificate signing request to send to Entrust. Be aware that at the time of this release, Entrust supports key modulus of size 1024 only. Consult Entrust if you are using any other value.

### Generate Certificate Signing Request Fields

- **Key Pair**—Use the drop-down menu to display the configured key pairs by name.
  - **Show**—Click to display information about the selected key pair, including date and time generated, usage (general or special purpose), modulus size, and key data.



- **New**—Click to add a new key pair, providing a name, modulus size, and usage. When you generate the key pair, you have the option of sending it to the security appliance or saving it to a file.
- **Certificate Subject DN**—Identifies DN attributes for the certificate.
  - **Common Name (CN)**—Enter the FQDN or IP address of the security appliance.
  - **Organization (O)**—Provide the name of the company.
  - **Country (C)**—Enter the two-letter code for the country.
- **Optional Parameters**—Lets you add additional attributes for the signing request.
  - **Additional DN Attributes**—These include Department (OU), State (ST), Location (L), and E-mail Address (EA).
  - **FQDN (SubjectAlt Name)**—Use this certificate extension field to enter additional fully qualified domain name information if the CA requires it.
- **Generate Request**—Click to generate the certificate signing request, which you can then **Send** to Entrust, or **Save to File**, and send later.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | •      |

## Installing Identity Certificates

The **Install** button on the Identity Certificates window is inactivated unless there is a pending enrollment. Whenever the security appliance receives a Certificate Signing Request (CSR), the Identity Certificates window displays the pending ID certificate. When you highlight the pending Identity Certificate, the Install button activates.

When you transmit the pending file to a CA, the CA enrolls it and returns a certificate to the security appliance. Once you have the certificate, click the Install button and highlight the appropriate Identity and CA certificates to complete the operation.

The following steps illustrate adding and installing a pending Identity Certificate:

### To Add the Identity Certificate:

- 
- Step 1** In the **Identity Certificates** panel, click the **Add** button.
  - Step 2** In the **Add Identity Certificate** panel, select **Add a new identity certificate**.
  - Step 3** Optionally, change the key pair or create a new key pair. A key pair is required.
  - Step 4** Enter the **Certificate Subject DN**: information and click the **Select...** button.
  - Step 5** In the **Certificate Subject DN** panel, be sure to specify all of the subject DN attributes required by the CA involved. See [Certificate Subject DN Attributes](#). Then click **OK** to close the **Certificate Subject DN** panel.
  - Step 6** In the **Add Identity Certificate** panel, click the **Advanced...** button.

- Step 7** In the **Advanced Options** panel, verify that the **FQDN:** field is the correct FQDN of the security appliance and click **OK** to close the window.
- Step 8** In the **Add Identity Certificate** panel, click the **Add Certificate** at the bottom.
- Step 9** When prompted to enter a name for the *CSR*, specify an easily-accessible file name of type text, such as *c:\verisign-csr.txt*.
- Step 10** Send the CSR text file to the CA. Alternatively, you can paste the text file into the CSR enrollment page on the CA's web site.

**To install an Identity Certificate:**

- Step 1** When the CA returns the Identity Certificate to you, return to the Identity Certificates panel, select the pending certificate entry, and click the now active **Install** button.
- Step 2** To assign the newly installed certificate for use with SSL VPN, navigate to the **SSL Settings** panel by SSL Settings hot link in the text under the list of certificates.
- Step 3** In the **SSL Settings** panel, double-click the interface to be assigned to the certificate. the **Edit SSL Certificate** panel opens.
- Step 4** In the **Edit SSL Certificate** panel, select the certificate from the **Certificate:** pull-down list and click **OK**. Note that the selected Identity Certificate displays in the **ID Certificate** field to the right of the selected **Interface** field.
- Step 5** Be sure to click the **Apply** button at the bottom of the **SSL Settings** panel to save the newly-installed certificate with the ASA configuration.

## Code-Signer Certificates

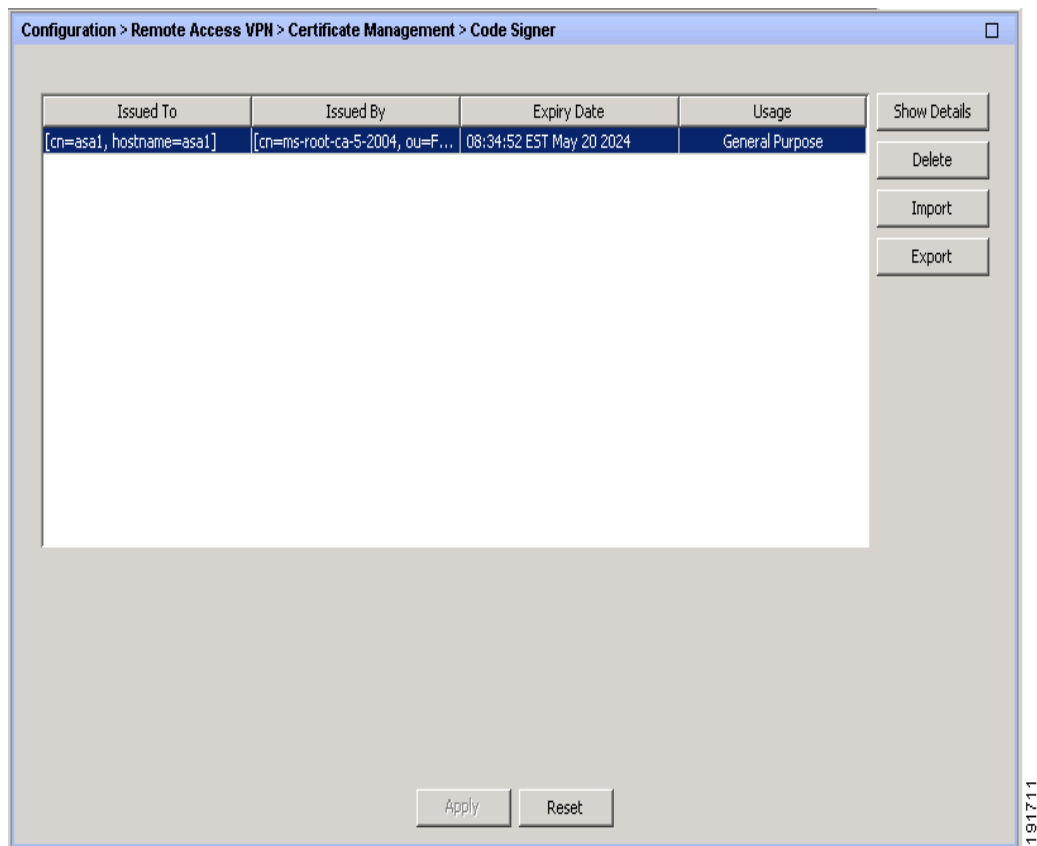
Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin. You can import code-signer certificates with the **Import** button on this panel or you can select the Java Code Signer panel, Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer.

The Code-signer Certificate Authentication panel allows you to:

- Display details of an Identity Certificate. See [Show Code-Signer Certificate Details](#).
- Delete an existing Identity Certificate. See [Delete a Code-Signer Certificate](#).

Export an existing Identity Certificate. See [Import or Export a Code-Signer Certificate](#).



### Show Code-Signer Certificate Details

The **Show Details** button displays the Code Signer Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.
- **Issued to**—Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.

### Delete a Code-Signer Certificate

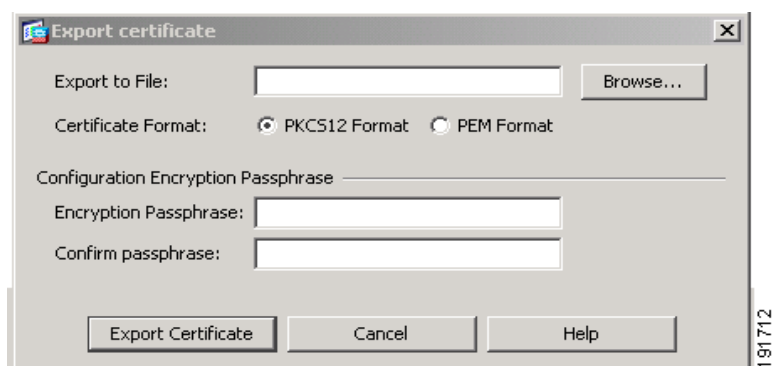
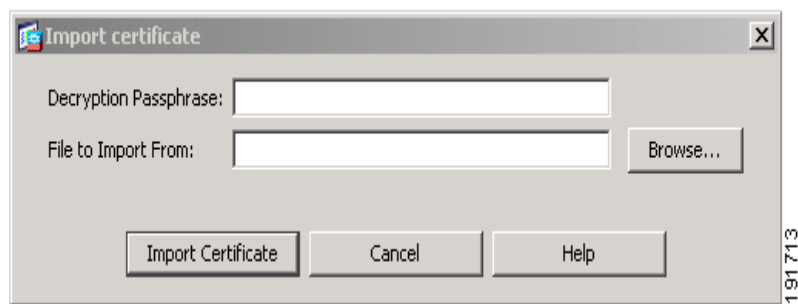
The **Delete** button immediately removes the selected Code Signer certificate configuration from the security appliance. Once you delete a configuration, it cannot be restored; to recreate the configuration, you must use the **Import** button to reenter the configuration information from the beginning



#### Note

Once you delete a Code Signer configuration, it cannot be restored.

### Import or Export a Code-Signer Certificate



Assign values to the fields in the **Import Certificate** window as follows:

- **Decryption Passphrase:** Specify the passphrase used to decrypt the PKCS12 file
- **Files to Import From:** You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the **Import Certificate** dialog box, which lets you navigate to the file containing the certificate.

Assign values to the fields in the **Export Certificate** window as follows:

- **Export to file**—Specify the name of the PKCS12-format file to use in exporting the certificate configuration;
- **Certificate Format:** Click **PKCS12 format**, the public key cryptography standard, which can be base64 encoded or hexadecimal, or click **PEM format**.
  - **Browse**—Display the **Select a File** dialog box that lets you navigate to the file to which you want to export the certificate configuration.
- **Decryption Passphrase**—Specify the passphrase used to decrypt the PKCS12 file for export.
  - **Confirm Passphrase**—Verify the decryption passphrase.
- **Export Certificate**—Exports the configuration.

## Local Certificate Authority

The Local Certificate Authority (CA) provides a secure configurable inhouse authority that resides the security appliance for certificate authentication.

**Note**

The local CA provides a certificate authority on the adaptive security appliance for use with SSL VPN connections, both browser- and client-based.

User enrollment is by browser webpage login. The Local CA integrates basic certificate authority functionality on the security appliance, deploys certificates, and provides secure revocation checking of issued certificates.

The following Local CA options allow you to initialize and set up the Local CA server and user database:

- Configure the Local CA Server on the security appliance. See [Configuring the Local CA Sever](#).
- Revoke/Unrevoke Local CA Certificates and update CRL. See [Manage User Certificates](#).
- Add, edit, and, delete Local CA users. See [Manage User Database](#).

## Default Local CA Server

The Local CA window displays the parameters to be configured for setting up a Local CA Server on the security appliance. The default characteristics of the initial Local CA server are listed in the following:

### Configurable Parameters

**Enable/Disable** buttons activate or deactivate the Local CA server.

The Enable passphrase secures the Local CA server from unauthorized or accidental shutdown

Certificate Issuer's Name

Issued certificate keypair size

Local CA Certificate key-pair size

Length of time the server certificate is valid

Length of time an issued user certificate

Simple Mail Transfer Protocol (SMTP) Server IP Address for Local CA e-mail

From-e-mail address that issues Local CA user certificate e-mail notices

Subject line in Local CA e-mail notices

More Options

Certificate Revocation List (CRL) Distribution Point (CDP), the location of the CRL on the Local CA security appliance

Length of time CRL is valid

Database Storage Location

Subject-name DN default to append to a username on issued certificates

Post-enrollment/renewal period for retrieving an issued certificate PKC12 file

Length of time a one-time password is valid

Days be expiration reminders are sent

### Defaults

Default is disabled. Select Enable to activate the Local CA server.

**Required - No default.** Supply a word with a minimum of seven alphanumeric characters)

`cn=hostname.domainname`

1024 bits per key

1024 bits per key

Server Certificate=3 yrs.

User Certificate=1 yr.

**Required - No default.** You supply the SMTP mail server IP address.

**Required - No default.** Supply an e-mail address in `adminname@host.com` format.

"Certificate Enrollment Invitation"

More Defaults

Specify the location of the CRL on the Local CA security appliance,

`http://hostname.domain/+CSCOCA+/asa_ca.crl`

CRL =6 hrs.

On-board flash memory

**Optional - No default.** Supply a subject-name default value.

24 hours

72 hrs. (three days)

14 days prior to certificate expiration.

**Configurable Parameters**

Length of time a one-time password is valid

**Defaults**

72 hrs. (three days)

**Caution:** Delete Certificate Authority Server button permanently removes the server configuration.

**Configuring the Local CA Sever**

The CA Server window lets you customize, modify, and control Local CA server operation. This section describes the parameters that can be specified. Additional parameters are available when you click **More Options**. See [More Local CA Configuration Options](#). For permanent removal of a configured Local CA, see [Deleting the Local CA Server](#). To customize the Local CA server, first review the initial settings shown in the preceding table.

**Note**

**Issuer-name** and **keysize server** values cannot be changed once you enable the Local CA. Be sure to review all optional parameters carefully before you enable the configured Local CA.

**Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**

Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority.

☐ Enable ☒ Disable

Issuer Name:

CA Server Key Size:

Client Key Size:

CA Certificate Lifetime:  days

Client Certificate Lifetime:  days

**SMTP Server & Email Settings**

Server IP Address:

From Address:

Subject:

**More Options**

CRL Distribution Point URL:

Publish-CRL Interface and Port:

CRL Lifetime:  hours

Database Storage Location:

Default Subject Name:

Enrollment Period:  hours

One Time Password Expiration:  hours

**Enable/Disable Buttons**

The **Enable/Disable** buttons activate or deactivate the Local CA server. Once you enable the Local CA server with the **Enable** button, the security appliance generates the Local CA server certificate, key pair and necessary database files.

The self-signed certificate key usage extension has key encryption, key signature, CRL signing, and certificate signing ability. The **Enable** button also archives the Local CA server certificate and key pair to storage in a PKCS12 file.

**Note**

Click **Apply** to be sure you save the Local CA certificate and key pair so the configuration is not lost if you reboot the security appliance.

When you select the **Disable** button to halt the Local CA server, you shutdown its operation on the security appliance. The configuration and all associated files remain in storage. Webpage enrollment is disabled while you change or reconfigure the Local CA.

**Passphrase**

When you enable the Local CA Server for the first time, you must provide an alphanumeric Enable passphrase. The passphrase protects the Local CA certificate and the Local CA certificate key pair archived in storage. The passphrase is required to unlock the PKCS12 archive if the Local CA certificate or key pair is lost and needs to be restored.

**Note**

There is no default for the enable passphrase; the passphrase is a required argument for enabling the Local CA Server. Be sure to keep a record of the enable passphrase in a safe place.

**Issuer Name**

The Certificate Issuer Name field contains the issuer's subject name dn, formed using the *username* and the subject-name-default DN setting as *cn=<FQDN>*. The Local CA server is the entity granting the certificate. The default certificate name is provided in the format: *cn=hostname.domainname*.

**CA Server Key Size**

The CA Key Size parameter is the size of the used for the server certificate generated for the Local CA server. Key size can be 512, 768, 1024, or 2048 bits per key. The default size is 1024 bits per key.

**Client Key Size**

The Key Size field specifies the size of the key pair to be generated for each user certificate issued by the Local CA server. Key size can be 512, 768, 1024, or 2048 bits per key. The default size is 1024 bits per key.

**CA Certificate Lifetime**

The **CA Certificate Lifetime** field specifies the length of time in days that the CA server certificate is valid. The default for the CA Certificate is 3650 days (10 years).

The Local CA Server automatically generates a replacement CA certificate 30 days prior to the CA certificate expiration, allowing the replacement certificate to be exported and imported onto any other devices for Local CA certificate validation of user certificates issued by the Local CA certificate after expiration. The pre-expiration Syslog message:

%ASA-1-717049: Local CA Server certificate is due to expire in <days> days and a replacement certificate is available for export.

**Note**

When notified of this automatic rollover, the administrator must take action to ensure the new Local CA certificate is imported to all necessary devices prior to expiration.

**Client Certificate Lifetime**

The **Client Certificate Lifetime** field specifies the length of time in days that a user certificate issued by the CA server is valid. The default for the CA Certificate is 365 days (one year).

### SMTP Server & Email Settings

To set up e-mail access for the Local CA server, you configure The Simple Mail Transfer Protocol (SMTP) e-mail server, the e-mail address from which to send e-mails to Local CA users, and you specify a standard subject line for Local CA e-mails.

- **Server IP Address** - The Server IP Address field requires the Local CA e-mail server's IP address. There is no default for the server IP address; you must supply the SMTP mail server IP address.
- **From Address** - The From Address field requires an e-mail address from which to send e-mails to Local CA users. Automatic e-mail messages carry one-time passwords to newly enrolled users and issue messages when certificates need to be renewed or updated. that issues Local CA user certificate e-mail notices. There is no From Address default value; you are required to supply an e-mail address in *adminname@host.com* format.
- **Subject** - The Subject field is a line of text specifying the subject line in all e-mails send to users by the Local CA server. If you do not specify a subject field, the default inserted by the Local CA server is "Certificate Enrollment Invitation".

### More Local CA Configuration Options

#### CRL Distribution Point URL

The Certificate Revocation List (CRL) Distribution Point (CDP) is the location of the CRL on the security appliance. The default CRL DP location is `http://hostname.domain/+CSCOCA+/asa_ca.crl`.

#### Publish CRL Interface and Port:

To make the CRL available for HTTP download on a given interface or port. Select an interface from the pull-down list. The optional port option can be any port number in a range of 1-65535. TCP port 80 is the HTTP default port number.

The CDP URL can be configured to utilize the IP address of an interface, and the path of the CDP URL and the file name can be configured also. (Note that you cannot rename the CRL; it always has the fixed name, LOCAL-CA-SERVER.crl.)

For example, the CDP URL could be configured to be: `http://10.10.10.100/user8/my_crl_file` In this case only the interface with that IP address works, and, when the request comes in, the security appliance matches the path `/user8/my_crl_file` to the configured CDP URL. When the path matches, the security appliance returns the CRL file stored in storage. Note that the protocol must be `http`, so the prefix is `http://`.

#### CRL Lifetime

The Certificate Revocation List (CRL) Lifetime field specifies the length of time in hours that the CRL is valid. The default for the CA Certificate is six hours.

The Local CA updates and reissues the CRL every time a user certificate is revoked or unrevoked, but if there are no revocation changes, the CRL is reissued once every CRL lifetime. You can force an immediate CRL update and list regeneration with the **CRL Issue** button on the Manage CA Certificates panel.

#### Database Storage Location

The Database Storage Location field allows you to specify a storage area for the Local CA configuration and data files. The security appliance accesses and implements user information, issued certificates, revocation lists, and so forth using a Local CA database.



That Local CA database resides can be configured to be on an off-box file system that is mounted and accessible to the security appliance. To specify an external file or share, enter the pathname to the external file or click **Browse** and search for the file.



**Note** Flash memory can store a database with 3500 users or less, but a database of more than 3500 users requires off-box storage.

### Default Subject Name

The Default Subject Name (DN) field allows you to specify a default subject name to append to a username on issued certificates. The permitted DN attribute keywords are listed in the following list:

| Default Subject-name-default DN Keywords |
|------------------------------------------|
| CN= Common Name                          |
| SN = Surname                             |
| O = Organization Name                    |
| L = Locality                             |
| C = Country                              |
| OU = Organization Unit                   |
| EA = E-mail Address                      |
| ST = State/Province                      |
| T = Title                                |

### Enrollment Period

The Enrollment Period field specifies the number of hours an enrolled user can retrieve a PKCS12 enrollment file in order to enroll and retrieve a user certificate. The enrollment period is independent of the OTP expiration period. The default Enrollment Period is 24 hours.



**Note** Certificate enrollment for the Local CA is supported only for Clientless SSL VPN connections and is not supported for other SSL VPN clients such as CVC or for IPSec VPN connections. For clientless SSL VPN connections, communications between the client and the head-end is through a web browser utilizing standard HTML.

### One-Time-Password Expiration

The One-Time-Password (OTP) expiration field specifies the length of time that a one-time password e-mailed to an enrolling user is valid. The default value is 72 hours.

### Certificate Expiration Reminder

The Certificate Expiration Reminder field specifies the number of days before expiration reminders are sent to e-mailed to users. The default is 14 days.

### Apply Button

The **Apply** button lets you save the new or modified CA certificate configuration.

**Reset Button**

The **Reset** button removes any changes or edits and returns the display to the original contents.

**Deleting the Local CA Server**

The **Delete Certificate Authority Server** button at the bottom of the **More Options** section of the **CA Server** panel, immediately removes the Local CA Certificate configuration from the security appliance. Once you delete the Local CA configuration, it cannot be restored; to recreate the deleted configuration, you must reenter the certificate configuration information from the beginning.

**Note**

Deleting the Local CA Server removes the configuration from the security appliance. Once deleted, the configuration is unrecoverable.

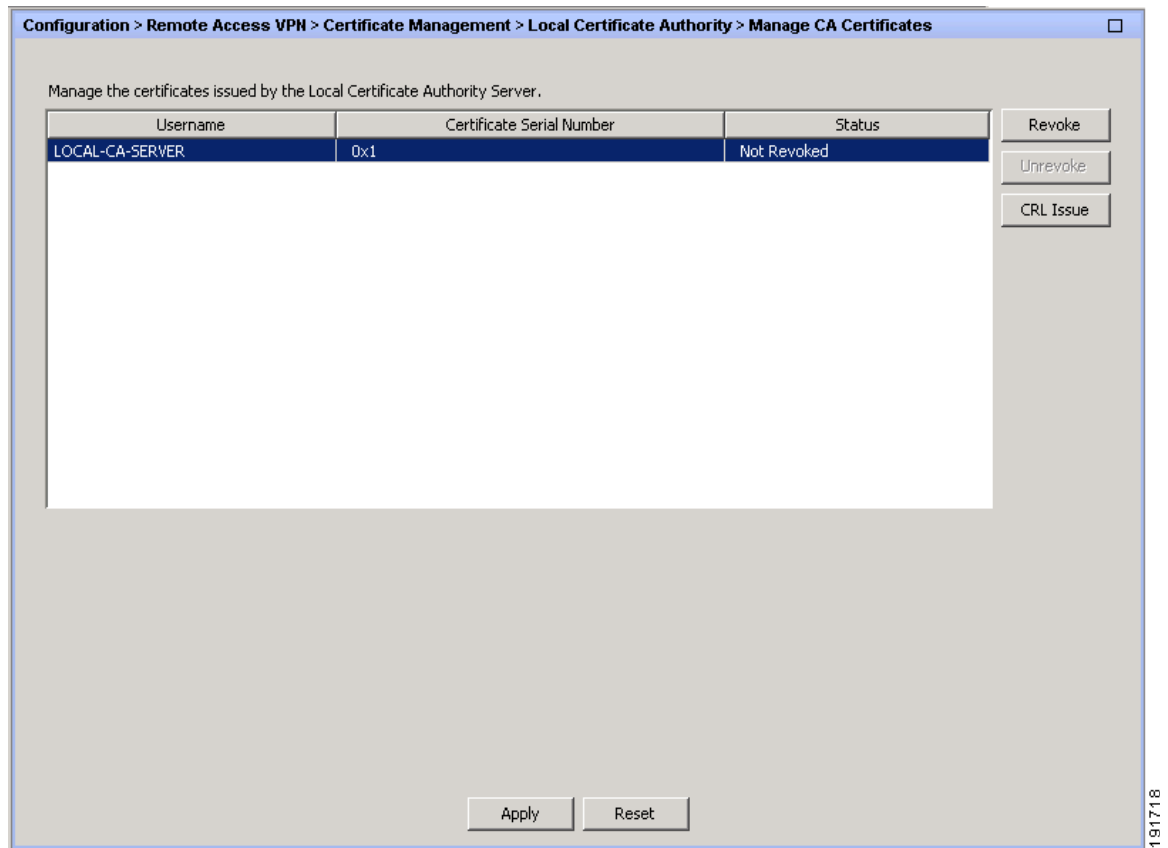
**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Manage User Certificates

The Local CA server maintains certificate renewals, re-issues user certificates, maintains the Certificate Revocation List (CRL), and revokes or restores privileges as needed. With the Manage User Certificates window, you can select specific certificates by username or by certificate serial number and change the certificate status (revoked/unrevoked).



Whenever you change any certificate status, be sure to update the CRL to reflect the latest changes.

- To change certificate status, see [Revoking a Local CA Certificate](#) and [Unrevoking a Local CA Certificate](#).

### Revoking a Local CA Certificate

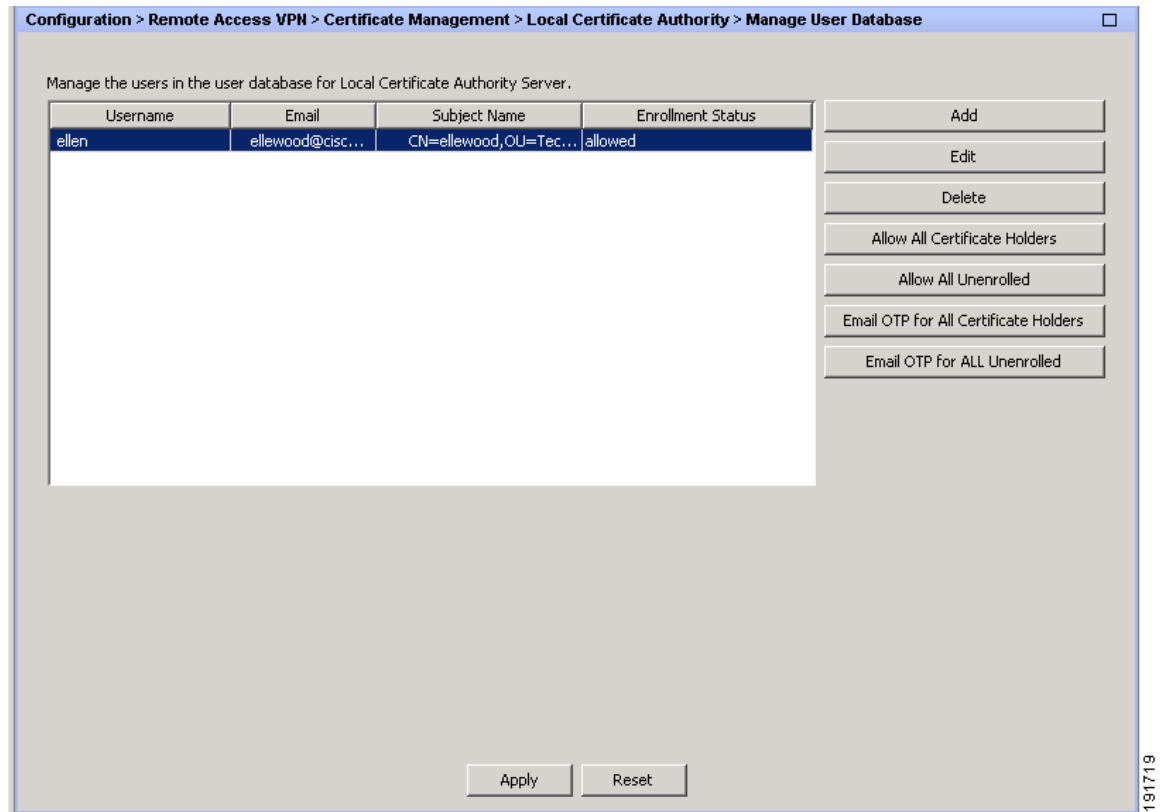
The Local CA Server keeps track of the lifetime of every user certificate and e-mails renewal notices when they are needed. If a user's certificate lifetime period runs out, that user's access is revoked. The Local CA also marks the certificate as revoked in the certificate database and automatically updates the information and reissues the CRL.

### Unrevoking a Local CA Certificate

An already revoked user certificate can have privileges restored with notification by e-mail. Select a revoked user's certificate and click Unrevoke to restore access. The Local CA also marks the certificate as unrevoke in the certificate database, automatically updates the certificate information, and reissues an updated CRL.

# Manage User Database

The Local CA user database contains user identification information and the status of each user in the system (enrolled, allowed, revoked, etc.). With the Manage User Database window, you can add new users, select specific users by username to edit user information, and you can delete existing users and their certificates.

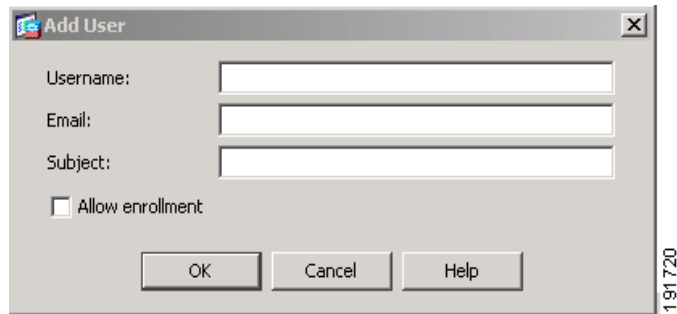


Whenever you add a user or modify any user's status, The Local CA automatically updates the CRL to reflect the latest changes.

- To add a user to the Local CA Database, see [Add a Local CA User](#).
- To change user identification information for an existing user, see [Edit a Local CA User](#).
- To remove a user from the database, see [Delete a Local CA User](#).
- To change the enrollment status of a user, see [Allow Enrollment](#).
- To e-mail One-Time-Passwords (OTPs) to a user, see [Email OTP](#).
- To view or regenerate a OTP, see [View/Re-generate OTP](#).

## Add a Local CA User

The **Add** button allows you to enter a new user into the Local CA database. Each new user to be entered into the database must have a predefined user name, e-mail address, and subject name.

A screenshot of the 'Add User' dialog box. It has a title bar with a close button. Inside, there are three text input fields labeled 'Username:', 'Email:', and 'Subject:'. Below these is a checkbox labeled 'Allow enrollment' which is currently unchecked. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.191720

### Local CA Add User Fields

- **Username:** Enter a valid user name.
- **Email:** Specify an existing valid e-mail address.
- **Subject:** Enter the user's subject name.

### Email OTP

The **Email OTP** button automatically sends an e-mail notice of enrollment permission with a unique one-time password (OTP) and the Local CA enrollment webpage URL to the newly added user.

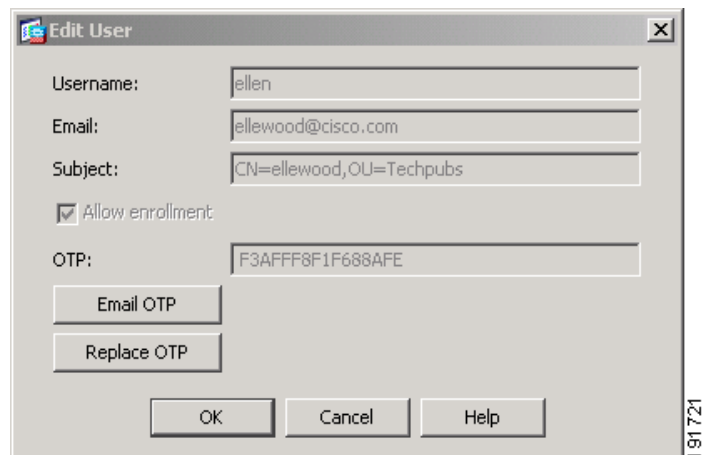
### Replace OTP

The **Replace OTP** button automatically reissues a new one-time password and sends an e-mail notice with the new password to the newly added user.

## Edit a Local CA User

The **Edit** button allows you to modify information on an existing Local CA user in the database. Select the specific user and click the **Edit** button.

You can modify the same fields as with the [Add a Local CA User](#) button. You can e-mail a new or replacement OTP to the user. Existing user information that can be modified includes user name, e-mail address, and subject name.

A screenshot of the 'Edit User' dialog box. It has a title bar with a close button. Inside, there are three text input fields labeled 'Username:', 'Email:', and 'Subject:'. The 'Username' field contains 'ellen', 'Email' contains 'ellewood@cisco.com', and 'Subject' contains 'CN=ellewood,OU=Techpubs'. Below these is a checkbox labeled 'Allow enrollment' which is checked. Below the checkbox is an 'OTP:' label and a text input field containing 'F3AFF8F1F688AFE'. Below the OTP field are two buttons: 'Email OTP' and 'Replace OTP'. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.191721

### Delete a Local CA User

The **Delete** button removes the selected user from the database and removes any certificates issued to that user from the Local CA Database. A deleted user cannot be restored; to recreate the deleted user record, you must use the **Add** button to reenter the user information.

### Allow Enrollment

The **Allow Enrollment** button enrolls the selected user.

### Email OTP

The **Email OTP** button sends an OTP to the selected user by email.

### View/Re-generate OTP

The **View/Re-generate OTP** button launches a window where you can regenerate the OTP of the selected user.



# CHAPTER 34

## 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 security appliance 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.

Here is some text marked print. Print is hidden.

## IKE Parameters

This panel lets you set system wide values for VPN connections. The following sections describe each of the options.

### Enabling IKE on Interfaces

You must enable IKE for each interface that you want to use for VPN connections.

### Enabling IPsec over NAT-T

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 disabled by default.

- The security appliance 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 security appliance 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:

- Open port 4500 on the security appliance.
- Enable IPsec over NAT-T globally in this panel.

- Select the second or third option for the Fragmentation Policy parameter in the **Configuration > VPN > IPsec > Pre-Fragmentation** panel. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

### Enabling 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 security appliance feature only. It does not work for LAN-to-LAN connections.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- The VPN 3002 hardware client, which supports one tunnel at a time, can connect using standard IPsec, IPsec over TCP, NAT-Traversal, or IPsec over UDP.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the security appliance 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 security appliance 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 security appliance. The client configuration must include at least one of the ports you set for the security appliance.

### Determining ID Method

During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:

|                  |                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>   | Uses the IP addresses of the hosts exchanging ISAKMP identity information.                                                                                                         |
| <b>Hostname</b>  | Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.                          |
| <b>Key ID</b>    | Uses the string the remote peer uses to look up the preshared key.                                                                                                                 |
| <b>Automatic</b> | Determines IKE negotiation by connection type: <ul style="list-style-type: none"> <li>• IP address for preshared key</li> <li>• Cert DN for certificate authentication.</li> </ul> |

### Disabling 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 information. This feature is disabled by default.



### Alerting Peers Before Disconnecting

Client or LAN-to-LAN sessions may be dropped for several reasons, such as: a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.

The security appliance can notify qualified peers (in LAN-to-LAN configurations), VPN Clients and VPN 3002 Hardware Clients 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 panel. This feature is disabled by default.

This panel lets you enable the feature so that the security appliance sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- Security appliance devices with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).
- VPN 3002 hardware clients running 4.0 or later software, and with Alerts enabled.
- VPN 3000 Series Concentrators running 4.0 or later software, with Alerts enabled.

### Waiting for Active Sessions to Terminate Prior to Reboot

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

### Fields

- **Enable IKE**—Shows IKE status for all configured interfaces.
  - **Interface**—Displays names of all configured security appliance interfaces.
  - **IKE Enabled**—Shows whether IKE is enabled for each configured interface.
  - **Enable/Disable**—Click to enable or disable IKE for the highlighted interface.
- **NAT Transparency**—Lets you enable or disable IPsec over NAT-T and IPsec over TCP.
  - **Enable IPsec over NAT-T**—Select to enable IPsec over NAT-T.
  - **NAT Keepalive**—Type the number of seconds that can elapse with no traffic before the security appliance terminates the NAT-T session. The default is 20 seconds. The range is 10 to 3600 seconds (one hour).
  - **Enable IPsec over TCP**—Select to enable IPsec over TCP.
  - **Enter up to 10 comma-separated TCP port values**—Type up to 10 ports on which to enable IPsec over TCP. Use a comma to separate the ports. You do not need to use spaces. The default port is 10,000. The range is 1 to 65,535.
- **Identity to Be Sent to Peer**—Lets you set the way that IPsec peers identify themselves to each other.
  - **Identity**—Select one of the following methods by which IPsec peers identify themselves:

|                  |                                                                                                                        |
|------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>   | Uses the IP addresses of the hosts.                                                                                    |
| <b>Hostname</b>  | Uses the fully-qualified domain names of the hosts. This name comprises the hostname and the domain name.              |
| <b>Key ID</b>    | Uses the string the remote peer uses to look up the preshared key.                                                     |
| <b>Automatic</b> | Determines IKE negotiation by connection type: IP address for preshared key or cert DN for certificate authentication. |

- **Key Id String**—Type the alpha-numeric string the peers use to look up the preshared key.
- **Disable inbound aggressive mode connections**—Select to disable aggressive mode connections.
- **Alert peers before disconnecting**—Select to have the security appliance notify qualified LAN-to-LAN peers and remote access clients before disconnecting sessions.
- **Wait for all active sessions to voluntarily terminate before rebooting**—Select to have the security appliance postpone a scheduled reboot until all active sessions terminate.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## IKE Policies

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.

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 security appliance uses this algorithm to derive the encryption and hash keys.
- A limit for how long the security appliance uses an encryption key before replacing it.

If you do not configure any IKE policies, the security appliance uses the default policy, which is always set to the lowest priority, and which contains the e 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

- **Policies**—Displays parameter settings for each configured IKE policy.

- **Priority #**—Shows the priority of the policy.
- **Encryption**—Shows the encryption method.
- **Hash**—Shows the has algorithm.
- **D-H Group**—Shows the Diffie-Hellman group.
- **Authentication**—Shows the authentication method.
- **Lifetime (secs)**—Shows the SA lifetime in seconds.
- **Add/Edit/Delete**—Click to add, edit, or delete an IKE policy.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit IKE Policy

### Fields

**Priority #**—Type a number to set a priority for the IKE policy. The range is 1 to 65,543, with 1 the highest priority.

**Encryption**—Select 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**—Select 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**—Select the authentication method the security appliance uses to establish the identity of each IPsec peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network. The choices follow:

|           |                  |
|-----------|------------------|
| pre-share | Pre-shared keys. |
|-----------|------------------|

|         |                                                                                                                                                                    |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rsa-sig | A digital certificate with keys generated by the RSA signatures algorithm.                                                                                         |
| crack   | IKE Challenge/Response for Authenticated Cryptographic Keys protocol for mobile IPsec-enabled clients which use authentication techniques other than certificates. |

**D-H Group**—Select 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)                                 |                                                                                                                        |
| 7 | Group 7 (Elliptical curve field size is 163 bits.) | Group 7 is for use with the Movian VPN client, but with any peer that supports Group 7 (ECC).                          |

**Lifetime (secs)**—Either select Unlimited or type an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the security appliance 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.

**Time Measure**—Select a time measure. The security appliance accepts the following values:

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

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Assignment Policy

IP addresses make internetwork connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network; and once that connection is made, the second set connects client and server through the VPN tunnel.

In security appliance address management, we are dealing with the second set of IP addresses: those private IP addresses that connect a client with a resource on the private network, through the tunnel, and let the client function as if it were directly connected to the private network. Furthermore, we are dealing

only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of security appliance management.

Therefore, when we discuss IP addresses here, we mean those IP addresses available in your private network addressing scheme, that let the client function as a tunnel endpoint.

The Assignment Policy panel lets you choose a way to assign IP addresses to remote access clients.

#### Fields

- **Use authentication server**—Select to assign IP addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IP addresses configured, we recommend using this method. Configure AAA servers on the **Configuration > AAA Setup** panels.
- **Use DHCP**— Select to obtain IP addresses from a DHCP server. If you use DHCP, configure the server on the **Configuration > DHCP Server** panel.
- **Use internal address pools**—Select to have the security appliance assign IP addresses from an internally configured 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 on **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** panel.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Address Pools

The IP Pool box shows each configured address pool by name, and with their IP address range, for example: 10.10.147.100 to 10.10.147.177. If no pools exist, the box is empty. The security appliance 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.

#### Fields

- **Pool Name**—Displays the name of each configured address pool.
- **Starting Address**—Shows first IP address available in each configured pool.
- **Ending Address**—Shows the last IP address available in each configured pool.
- **Subnet Mask**—Shows the subnet mask for addresses in each configured pool.
- **Add**—Click to add a new address pool.
- **Edit/Delete**—Click to edit or delete an already configured address pool.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit IP Pool

These panels let you:

- Add a new pool of IP addresses from which the security appliance assigns addresses to clients.
- Modify an IP address pool that you have previously configured.

The IP addresses in the pool range must not be assigned to other network resources.

### Fields

- **Name**—Assign an alpha-numeric name to the address pool. Limit 64 characters
- **Starting IP Address**—Enter the first IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.100.
- **Ending IP Address**—Enter the last IP address available in this pool. Use dotted decimal notation, for example: 10.10.147.100.
- **Subnet Mask**—Select the subnet mask for the IP address pool.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

# IPsec

IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPsec.

In IPsec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment with IPsec, 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).

In IPsec LAN-to-LAN connections, the security appliance can function as initiator or responder. In IPsec client-to-LAN connections, the security appliance 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 VPN Client complies with the IPsec protocol and is specifically designed to work with the security appliance. However, the security appliance can establish IPsec connections with many protocol-compliant clients. Likewise, the security appliance can establish LAN-to-LAN connections with other protocol-compliant VPN devices, often called secure gateways.

This security appliance 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
- Diffie-Hellman Groups 1, 2, 5, and 7
- Encryption Algorithms:
  - AES-128, -192, and -256
  - 3DES-168
  - DES-56
  - ESP-NUL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

## Crypto Maps

This pane shows the currently configured crypto maps, including the IPsec rules. Use it to add, edit, delete and move up, move down, cut, copy, and paste an IPsec rule.

### Fields



#### Note

You cannot edit, delete, or copy an implicit rule. The security appliance 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.

- **Add**—Click to launch the Add IPsec Rule dialog, where you can configure basic, advanced, and traffic selection parameters for a rule, or choose
- **Edit**—Click to edit an existing rule.
- **Delete**—Click to delete a rule highlighted in the table.
- **Cut**—Deletes a highlighted rule in the table and keeps it in the clipboard for copying.

- **Copy**—Copies a highlighted rule in the table.
- **Find**—Click to enable the Find toolbar where you can specify the parameters of existing rules that you want to find:
  - **Filter**—Filter the find results 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 that displays all existing entries that you can choose.
- **Diagram**—Displays a diagram that illustrates the highlighted IPsec rule.
- **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 security appliance maps the inside host's address to an address from the pool. After a host creates an outbound connection, the security appliance 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 is enabled for the policy.
- **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 the ["Rule Actions > QoS Tab"](#) section on page 21-26) 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 become false alarms in the case of priority queueing. Configuring the anti-replay window size helps you avoid possible false alarms.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Create 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 panel 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.

### Fields

- **Interface**—Select the interface name to which this policy applies.
- **Policy Type**—Select the type, static or dynamic, of this tunnel policy.
- **Priority**—Enter the priority of the policy.
- **Transform Set to Be Added**—Select the 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 transform sets in the list box. You can add a maximum of 11 transform sets 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.) Select bidirectional, originate-only, or answer-only to specify the connection type of this policy. For LAN-to-LAN connections, select bidirectional or answer-only (not originate-only). Select answer-only for LAN-to-LAN redundancy.
  - **IP Address of Peer to Be Added**—Enter the IP address of the IPsec peer you are adding.
- **Enable Perfect Forward 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 select a Diffie-Hellman group which the security appliance 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 7 (ECC) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 7 (ECC) to generate IPsec session keys, where the elliptic curve field size is 163 bits. This option is the fastest and requires the least overhead. It is intended for use with the Movian VPN client, but you can use it with any peers that support Group 7 (ECC).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Create IPsec Rule/Tunnel Policy (Crypto Map) - Advanced Tab

### Fields

- **Security Association Lifetime** parameters—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.
- **Enable NAT-T**— Enables NAT Traversal (NAT-T) for this policy.

- **Enable Reverse Route Injection**—Enables Reverse Route Injection for this policy.
- **Static Type Only Settings**—Specifies parameters for static tunnel policies.
  - **CA Certificate**—Selects the certificate to use. If you select something other than None (Use Preshared Keys), which is the default, the Enable entire chain transmission check box becomes active.
  - **Enable entire chain transmission**—Enables transmission of the entire trust point chain.
  - **IKE Negotiation Mode**—Selects 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 select Aggressive, the Diffie-Hellman Group list becomes active.
  - **Diffie-Hellman Group**—Select the Diffie-Hellman group to apply. The choices are as follows: Group 1 (768-bits), Group 2 (1024-bits), Group 5 (1536-bits), Group 7 (ECC).

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Create IPsec Rule/Traffic Selection Tab

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

### Fields

- **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 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**—Selects a standard subnet mask to apply to the IP address. This parameter appears when you select 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 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**—Selects a standard subnet mask to apply to the IP address. This parameter appears when you select 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 window where you can select 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 window where you can select 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**—Selects the interface name for the IP address. This parameter appears when you select the IP Address option button.
  - **IP address**—Specifies the IP address of the interface to which this policy applies. This parameter appears when you select 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 dialogs that contain the following fields:
    - **Name**—Selects the interface name to use as the source or destination host or network. This parameter appears when you select the Name option button. This is the only parameter associated with this option.
    - **Interface**—Selects the interface name for the IP address. This parameter appears when you select the Group option button.
    - **Group**—Selects 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 select 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 panel, 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 selected 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, kerberos, 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 select 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)—Selects 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.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Pre-Fragmentation

Use this panel to set the IPsec pre-fragmentation policy and do-not-fragment (DF) bit policy for any interface.

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 security appliance and the client rejects or drops IP fragments. For example, suppose a client wants to FTP get from an FTP server behind a security appliance. The FTP server transmits packets that when encapsulated would exceed the security appliance's MTU size on the public interface. The selected options determine how the security appliance processes these packets. The pre-fragmentation policy applies to all traffic travelling out the security appliance public interface.

The security appliance encapsulates all tunneled packets. After encapsulation, the security appliance 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 security appliance fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the security appliance 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 security appliance 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.

### Fields

- **Pre-Fragmentation**—Shows the current pre-fragmentation configuration for every configured interface.
  - **Interface**—Shows the name of each configured interface.
  - **Pre-Fragmentation Enabled**—Shows, for each interface, whether pre-fragmentation is enabled.
  - **DF Bit Policy**—Shows the DF Bit Policy for each interface.
- **Edit**—Displays the Edit IPsec Pre-Fragmentation Policy dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit IPsec Pre-Fragmentation Policy

Use this panel to modify an existing IPsec pre-fragmentation policy and do-not-fragment (DF) bit policy for an interface selected on the parent panel, **Configuration > VPN > IPsec > Pre-Fragmentation**

### Fields

- **Interface**—Identifies the selected interface. You cannot change this parameter using this dialog box.
- **Enable IPsec pre-fragmentation**—Enables or disables IPsec pre-fragmentation. The security appliance fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the security appliance 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**—Selects the do-not-fragment bit policy: Copy, Clear, or Set.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## IPsec Transform Sets

Use this panel to view and add or edit 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).

### Fields

- **Transform Sets**—Shows the configured transform sets.
  - **Name**—Shows the name of the transform sets.
  - **Mode**—Shows the mode, Tunnel, of the transform set. This parameter specifies the mode for applying ESP encryption and authentication; in other words, what part of the original IP packet has ESP applied. 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.

- **ESP Encryption**—Shows the 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**—Shows the ESP authentication algorithms for the transform sets.
- **Add**—Opens the Add Transform Set dialog box, in which you can add a new transform set.
- **Edit**—Opens the Edit Transform Set dialog box, in which you can modify an existing transform set.
- **Delete**—Removes the selected transform set. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Transform Set

Use this panel to add or modify a transform set. 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).

### Fields

- **Set Name**—Specifies a name for this transform set.
- **Properties**—Configures properties for this transform set. These properties appear in the Transform Sets table.
  - **Mode**—Shows the mode, Tunnel, of the transform set. This field shows the mode for applying ESP encryption and authentication; in other words, what part of the original IP packet has ESP applied. 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.
  - **ESP Encryption**—Selects the 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**—Selects the ESP authentication algorithms for the transform sets.



### Note

The IPsec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity.”

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Load Balancing



### Note

To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

This window lets you enable load balancing on the security appliance. Enabling load balancing involves:

- Configuring the load-balancing cluster by establishing a common virtual cluster IP address, UDP port (if necessary), and IPsec shared secret for the cluster. These values are identical for every device in the cluster.
- Configuring the participating device by enabling load balancing on the device and defining device-specific properties. These values vary from device to device.

If you have a remote-client configuration in which you are using two or more security appliances connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called *load balancing*. 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 and availability.



### Note

Load balancing is effective only on remote sessions initiated with the Cisco VPN Client (Release 3.0 and later), the Cisco VPN 3002 Hardware Client (Release 3.5 and later), or the ASA 5505 operating as an Easy VPN Client. All other clients, including LAN-to-LAN connections, can connect to a security appliance on which load balancing is enabled, but cannot participate in load balancing.

To implement load balancing, you group together logically two or more devices on the same private LAN-to-LAN network into a *virtual cluster*.

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

The virtual cluster appears to outside clients as a single *virtual cluster IP address*. This IP address is not tied to a specific physical device. It belongs to the current virtual cluster master; hence, it is virtual. A VPN client attempting to establish a connection connects first to this virtual cluster IP address. The

virtual cluster master then sends back to the client the public IP address of the least-loaded available host in the cluster. In a second transaction (transparent to the user) the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

**Note**

All clients other than the Cisco VPN client, the Cisco VPN 3002 Hardware Client, or the ASA 5505 operating as an Easy VPN Client connect directly to the security appliance as usual; they do not use the virtual cluster IP address.

If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to another active device in the cluster. Should the virtual cluster master itself fail, a secondary device in the cluster immediately and automatically takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

**Prerequisites**

Load balancing is disabled by default. You must explicitly enable load balancing.

You must have first configured the public and private interfaces and also have previously configured the interface to which the virtual cluster IP address refers.

All devices that participate in a cluster must share the same cluster-specific values: IP address, encryption settings, encryption key, and port. All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

**Fields**

- **VPN Load Balancing**—Configures virtual cluster device parameters.
  - **Participate in Load Balancing Cluster**—Specifies that this device is a participant in the load-balancing cluster.
  - **VPN Cluster Configuration**—Configures device parameters that must be the same for the entire virtual cluster. All servers in the cluster must have an identical cluster configuration.
  - **Cluster IP Address**—Specifies the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the security appliances 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.
  - **Enable IPsec Encryption**—Enables or disables IPsec encryption. If you select this check box, you must also specify and verify a shared secret. The security appliances 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, select this check box.

**Note**

When using encryption, you must have previously configured the load-balancing inside interface. If that interface is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.

If the load-balancing inside interface was enabled when you configured cluster encryption, but was disabled before you configured the participation of the device in the virtual cluster, you get an error message when you select the Participate in Load Balancing Cluster check box, and encryption is not enabled for the cluster.

- **IPsec Shared Secret**—Specifies the shared secret to between IPsec peers when you have enabled IPsec encryption. The value you enter in the box appears as consecutive asterisk characters.
- **Verify Secret**—Confirms the shared secret value entered in the IPsec Shared Secret box.
- **VPN Server Configuration**—Configures parameters for this specific device.
  - **Interfaces**—Configures the public and private interfaces and their relevant parameters.
  - **Public**—Specifies the name or IP address of the public interface for this device.
  - **Private**—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 secondary 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 IP Address**—Specifies the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used or if the device is not behind a firewall using NAT.
- **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.

To enable Clientless SSL VPN load balancing using FQDNs rather than IP addresses, you must do the following configuration steps:

- 
- Step 1** Enable the use of FQDNs for Load Balancing by checking the Send FQDN to client... checkbox.
  - Step 2** Add an entry for each of your security appliance outside interfaces into your DNS server, if such entries are not already present. Each security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup.
  - Step 3** Enable DNS lookups on your security appliance on the dialog box Configuration > Device Management > DNS > DNS Client for whichever interface has a route to your DNS server.
  - Step 4** Define your DNS server IP address on the security appliance. To do this, click Add on this dialog box. This opens the Add DNS Server Group dialog box. Enter the IP address of the DNS server you want to add; for example, 192.168.1.1 (IP address of your DNS server).
  - Step 5** Click OK and Apply.
- 

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Setting Global NAC Parameters

The security appliance uses Extensible Authentication Protocol (EAP) over UDP (EAPoUDP) messaging to validate the posture of remote hosts. Posture validation involves the checking of a remote host for compliance with safety requirements before the assignment of a network access policy. An Access Control Server must be configured for Network Admission Control before you configure NAC on the security appliance.

### Fields

The NAC window lets you set attributes that apply to all NAC communications. The following global attributes at the top of the window apply to EAPoUDP messaging between the security appliance and remote hosts:

- **Port**—Port number for EAP over UDP communication with the Cisco Trust Agent (CTA) on the host. This number must match the port number configured on the CTA. Enter a value in the range 1024 to 65535. The default setting is 21862.
- **Retry if no response**—Number of times the security appliance resends an EAP over UDP message. This attribute limits the number of consecutive retries sent in response to Rechallenge Interval expirations. The setting is in seconds. Enter a value in the range 1 to 3. The default setting is 3.
- **Rechallenge Interval**—The security appliance starts this timer when it sends an EAPoUDP message to the host. A response from the host clears the timer. If the timer expires before the security appliance receives a response, it resends the message. The setting is in seconds. Enter a value in the range 1 to 60. The default setting is 3.
- **Wait before new PV Session**—The security appliance starts this timer when it places the NAC session for a remote host into a hold state. It places a session in a hold state if it does not receive a response after sending EAPoUDP messages equal to the value of the “Retry if no response” setting. The security appliance also starts this timer after it receives an Access Reject message from the ACS server. When the timer expires, the security appliance tries to initiate a new EAP over UDP association with the remote host. The setting is in seconds. Enter a value in the range 60 to 86400. The default setting is 180.

The Clientless Authentication area of the NAC window lets you configure settings for hosts that are not responsive to the EAPoUDP requests. Hosts for which there is no CTA running do not respond to these requests.

- **Enable clientless authentication**—Click to enable clientless authentication. The security appliance sends the configured clientless username and password to the Access Control Server in the form of a user authentication request. The ACS in turn requests the access policy for clientless hosts. If you leave this attribute blank, the security appliance applies the default ACL for clientless hosts.
- **Clientless Username**—Username configured for clientless hosts on the ACS. The default setting is clientless. Enter 1 to 64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), single and double quotation marks (“ ” and "), asterisks (\*), and angle brackets (< and >).

- **Password**—Password configured for clientless hosts on the ACS. The default setting is clientless. Enter 4 – 32 ASCII characters.
- **Confirm Password**—Password configured for clientless hosts on the ACS repeated for validation.
- **Enable Audit**—Click to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server, such as a Trend server, uses the host IP address to challenge the host directly to assess its health. For example, it may challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host.
- **None**—Click to disable clientless authentication and audit services.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Network Admission Control Policies

The NAC Policies table displays the Network Admission Control (NAC) policies configured on the security appliance.

To add, change, or remove a NAC policy, do one of the following:

- To add a NAC policy, choose **Add**. The Add NAC Framework Policy dialog box opens.
- To change a NAC policy, double-click it, or select it and click **Edit**. The Edit NAC Framework Policy dialog box opens.
- To remove a NAC policy, select it and click **Delete**.

The following sections describe NAC, its requirements, and how to assign values to the policy attributes:

- [About NAC](#)
- [Uses, Requirements, and Limitations](#)
- [Fields](#)
- [What to Do Next](#)

### About NAC

NAC protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network. We refer to these checks as *posture validation*. You can configure posture validation to ensure that the anti-virus files, personal firewall rules, or intrusion protection software on a host with an AnyConnect or Clientless SSL VPN session are up-to-date before providing access to vulnerable hosts on the intranet. Posture validation can include the verification that the applications

running on the remote hosts are updated with the latest patches. NAC occurs only after user authentication and the setup of the tunnel. NAC is especially useful for protecting the enterprise network from hosts that are not subject to automatic network policy enforcement, such as home PCs.

The establishment of a tunnel between the endpoint and the security appliance triggers posture validation.

You can configure the security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server, such as a Trend server, uses the host IP address to challenge the host directly to assess its health. For example, it may challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host.

Following successful posture validation or the reception of a token indicating the remote host is healthy, the posture validation server sends a network access policy to the security appliance for application to the traffic on the tunnel.

In a *NAC Framework* configuration involving the security appliance, only a Cisco Trust Agent running on the client can fulfill the role of posture agent, and only a Cisco Access Control Server (ACS) can fulfill the role of posture validation server. The ACS uses dynamic ACLs to determine the access policy for each client.

As a RADIUS server, the ACS can authenticate the login credentials required to establish a tunnel, in addition to fulfilling its role as posture validation server.



#### Note

Only a NAC Framework policy configured on the security appliance supports the use of an audit server.

In its role as posture validation server, the ACS uses access control lists. If posture validation succeeds and the ACS specifies a redirect URL as part of the access policy it sends to the security appliance, the security appliance redirects all HTTP and HTTPS requests from the remote host to the redirect URL. Once the posture validation server uploads an access policy to the security appliance, all of the associated traffic must pass both the Security Appliance and the ACS (or vice versa) to reach its destination.

The establishment of a tunnel between a remote host and the security appliance triggers posture validation if a NAC Framework policy is assigned to the group policy. The NAC Framework policy can, however, identify operating systems that are exempt from posture validation and specify an optional ACL to filter such traffic.

## Uses, Requirements, and Limitations

When configured to support NAC, the security appliance functions as a client of a Cisco Secure Access Control Server, requiring that you install a minimum of one Access Control Server on the network to provide NAC authentication services.

Following the configuration of one or more Access Control Servers on the network, you must register the Access Control Server group, using the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit External** menu option. Then add the NAC policy.

ASA support for NAC Framework is limited to remote access IPsec and Clientless SSL VPN sessions. The NAC Framework configuration supports only single mode.

NAC on the ASA does not support Layer 3 (non-VPN) and IPv6 traffic.

### Fields

- Policy Name—Enter a string of up to 64 characters to name the new NAC policy.

Following the configuration of the NAC policy, the policy name appears next to the NAC Policy attribute in the Network (Client) Access group policies. Assign a name that will help you to distinguish its attributes or purpose from others that you may configure.

- **Status Query Period**—The security appliance starts this timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a *status query*. Enter the number of seconds in the range 30 to 1800. The default setting is 300.
- **Revalidation Period**—The security appliance starts this timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The security appliance maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation. Enter the interval in seconds between each successful posture validation. The range is 300 to 86400. The default setting is 36000.
- **Default ACL**— (Optional) The security appliance applies the security policy associated with the selected ACL if posture validation fails. Select None or select an extended ACL in the list. The default setting is None. If the setting is None and posture validation fails, the security appliance applies the default group policy.

Use the Manage button to populate the drop-down list and view the configuration of the ACLs in the list.

- **Manage**— Opens the ACL Manager dialog box. Click to view, enable, disable, and delete standard ACLs and the ACEs in each ACL. The list next to the Default ACL attribute displays the ACLs.
- **Authentication Server Group**—Specifies the authentication server group to use for posture validation. The drop-down list next to this attribute displays the names of all server groups of type RADIUS configured on this security appliance that are available for remote access tunnels. Select an ACS group consisting of at least one server configured to support NAC.
- **Posture Validation Exception List**—Displays one or more attributes that exempt remote computers from posture validation. At minimum, each entry lists the operating system and an Enabled setting of Yes or No. An optional filter identifies an ACL used to match additional attributes of the remote computer. An entry that consists of an operating system and a filter requires the remote computer to match both to be exempt from posture validation. The security appliance ignores the entry if the Enabled setting is set to No.
- **Add**—Adds an entry to the Posture Validation Exception list.
- **Edit**—Modifies an entry in the Posture Validation Exception list.
- **Delete**—Removes an entry from the Posture Validation Exception list.

## What to Do Next

Following the configuration of the NAC policy, you must assign it to a group policy for it to become active. To do so, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > General > More Options** and the NAC policy name from the drop-down list next to the NAC Policy attribute.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Posture Validation Exception

The Add/Edit Posture Validation Exception dialog window lets you exempt remote computers from posture validation, based on their operating system and other optional attributes that match a filter.

- **Operating System**—Choose the operating system of the remote computer. If the computer is running this operating system, it is exempt from posture validation. The default setting is blank.
- **Enable**—The security appliance checks the remote computer for the attribute settings displayed in this window only if you check Enabled. Otherwise, it ignores the attribute settings. The default setting is unchecked.
- **Filter**— (Optional) Use to apply an ACL to filter the traffic if the operating system of the computer matches the value of the Operating System attribute.
- **Manage**— Opens the ACL Manager dialog box. Click to view, enable, disable, and delete standard ACLs and the ACEs in each ACL. The list next to the Default ACL attribute displays the ACLs. Use this button to populate the list next to the Filter attribute.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |





# CHAPTER 35

## General

---

A virtual private network is a network of virtual circuits that carry private traffic over a public network such as the Internet. VPNs can connect two or more LANS, or remote users to a LAN. VPNs provide privacy and security by requiring all users to authenticate and by encrypting all data traffic.

## Client Software

The **Client Software** pane lets administrators at a central location do the following actions:

- Enable client update; specify the types and revision numbers of clients to which the update applies.
- Provide a URL or IP address from which to get the update.
- In the case of Windows clients, optionally notify users that they should update their VPN client version.



### Note

The Client Update function at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software applies only to the IPsec VPN client, (For Windows, MAC OS X, and Linux), and the VPN 3002 hardware client. It does not apply to the Cisco AnyConnect VPN clients, which is updated by the security appliance automatically when it connects.

For the IPsec VPN client, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. You can apply client updates only to the IPsec remote-access tunnel-group type.



### Note

If you try to do a client update to an IPsec Site-to-Site IPsec connection or a Clientless VPN IPsec connection, you do not receive an error message, but no update notification or client update goes to those types of IPsec connections.

To enable client update globally for all clients of a particular client type, use this window. You can also notify all Windows, MAC OS X, and Linux clients that an upgrade is needed and initiate an upgrade on all VPN 3002 hardware clients from this window. To configure the client revisions to which the update applies and the URL or IP address from which to download the update, click Edit.

To configure client update revisions and software update sources for a specific tunnel group, see Configuration > Remote Access VPN > Network (Client) Access > IPsec > Add/Edit > Advanced > IPsec > Client Software Update.

**Fields**

- **Enable Client Update**—Enables or disables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.
- **Client Type**—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows 95, 98 or ME and Windows NT, 2000 or XP individually. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.
- **VPN Client Revisions**—Contains a comma-separated list of software image revisions appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
  - The revision list must include the software version for this update.
  - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
  - The TFTP server for distributing the hardware client image must be a robust TFTP server.
  - A VPN client user must download an appropriate software version from the listed URL.
  - The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.
- **Image URL**—Contains the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: `http://` or `https://`. For hardware clients, the URL must be in the form `tftp://`.
  - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is:  
`http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:  
`http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe`  
The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.
  - For the hardware client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:  
`tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin`
- **Edit**—Opens the Edit Client Update Entry dialog box, which lets you configure or change client update parameters. See [Edit Client Update Entry](#).
- **Live Client Update**—Sends an upgrade notification message to all currently connected VPN clients or selected tunnel group(s).
  - **Tunnel Group**—Selects all or specific tunnel group(s) for updating.
  - **Update Now**—Immediately sends an upgrade notification containing a URL specifying where to retrieve the updated software to the currently connected VPN clients in the selected tunnel group or all connected tunnel groups. The message includes the location from which to download the new version of software. The administrator for that VPN client can then retrieve the new software version and update the VPN client software.

For VPN 3002 hardware clients, the upgrade proceeds automatically, with no notification.

You must check Enable Client Update in the window for the upgrade to work. Clients that are not connected receive the upgrade notification or automatically upgrade the next time they log on.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Edit Client Update Entry

The Edit Client Update dialog box lets you change information about VPN client revisions and URLs for the indicated client types. The clients must be running one of the revisions specified for the indicated client type. If not, the clients are notified that an upgrade is required.

### Fields

- Client Type—(*Display-only*) Displays the client type selected for editing.
- VPN Client Revisions—Lets you type a comma-separated list of software or firmware images appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client. If the client is not running a software version on the list, an update is in order. The user of a Windows, MAC OS X, or Linux-based VPN client must download an appropriate software version from the listed URL. The VPN 3002 hardware client software is automatically updated via TFTP.
- Image URL—Lets you type the URL for the software/firmware image. This URL must point to a file appropriate for this client.

- For a Windows, MAC OS X, or Linux-based VPN client, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: `http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.

- For the hardware client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```

The directory is optional.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Default Tunnel Gateway

To configure the default tunnel gateway, click the Static Route link in this window. The Configuration > Routing > Routing > Static Route window opens.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Group Policies

The Group Policies window lets you manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS or LDAP server. Configuring the VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts.

The “child” windows and dialog boxes let you configure the group parameters, including those for the default group. The default group parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. 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 either an internal or an external group policy. An internal group policy is stored locally, and an external group policy is stored externally on a RADIUS or LDAP server. Clicking Edit opens a similar dialog box on which you can create a new group policy or modify an existing one.

In these 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, SSL VPN Client and AnyConnect Client, and IPsec Client.

Before configuring these parameters, you should configure:

- Access hours.
- Rules and filters.

- IPsec Security Associations.
- Network lists for filtering and split tunneling
- User authentication servers, and specifically the internal authentication server.

#### Fields

- **Group Policy**—Lists the currently configured group policies and Add, Edit, and Delete buttons to help you manage VPN group policies.
  - **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.
  - **AAA Server Group**—Lists the AAA server group, if any, to which each currently configured group policy pertains.
  - **Add**—Offers a drop-down menu on which you can select 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. Offers a drop-down menu on which you can select whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy.
  - **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.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit External Group Policy

The Add or Edit External Group Policy dialog box lets you configure an 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.
- **Password**—Specifies the password for this server group policy.
- **New**—Opens a dialog box that lets you select 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add AAA Server Group

The Add AAA Server Group dialog box lets you configure a new AAA server group. The Accounting Mode attribute applies only to RADIUS and TACACS+ protocols.

### Fields

- **Server Group**—Specifies the name of the server group.
- **Protocol**—(*Display only*) Indicates whether this is a RADIUS or an LDAP server group.
- **Accounting Mode**—Indicates whether to use simultaneous or single accounting mode. In single mode, the security appliance sends accounting data to only one server. In simultaneous mode, the security appliance sends accounting data to all servers in the group. The Accounting Mode attribute applies only to RADIUS and TACACS+ protocols.
- **Reactivation Mode**—Specifies the method by which failed servers are reactivated: Depletion or Timed reactivation mode. In Depletion mode, failed servers are reactivated only after all of the servers in the group become inactive. In Timed mode, failed servers are reactivated after 30 seconds of down time.
- **Dead Time**—Specifies, for depletion mode, the number of minutes (0 through 1440) that must elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. The default value is 10 minutes. This field is not available for timed mode.
- **Max Failed Attempts**— Specifies the number (an integer in the range 1 through 5) of failed connection attempts allowed before declaring a nonresponsive server inactive. The default value is 3 attempts.

## Adding or Editing a Remote Access Internal Group Policy, General Attributes

The Add or Edit Group Policy window lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields on this window, 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 on this dialog box.

### Fields

The following attributes appear in the Add Internal Group Policy > General window. They apply to SSL VPN and IPSec sessions, or clientless SSL VPN 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.
- **Banner**—Specifies the banner text to present to users at login. The length can be up to 491 characters. There is no default value.

- **Address Pools**—(Network (Client) Access only) Specifies the name of one or more address pools to use for this group policy.
- **Select**—(Network (Client) Access only) Opens the Select Address Pools window, which shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you select, add, edit, delete, and assign entries from that list.
- **More Options**—Displays 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 a security appliance; 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.
  - **IPSec**—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 client-to-LAN connections can use IPSec.
  - **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.



---

**Note** If you do not select a protocol, an error message appears.

---

- **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 security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Group Policy window.
- **Web ACL**—(Clientless SSL VPN only) Select an access control list (ACL) from the drop-down list if you want to filter traffic. Click **Manage** next to the list if you want to view, modify, add, or remove ACLs before making a selection.
- **Manage**—Displays the ACL Manager window, with which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs). For more information about the ACL Manager, see the online Help for that window.
- **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 selected, the default value is --Unrestricted--.

- **Manage**—Opens the Browse Time Range dialog box, on 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 security appliance forwards all traffic on 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 on this security appliance.



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

- **Maximum Connect Time**—If the Inherit check box is not selected, this parameter specifies the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 35791394 minutes (over 4000 years). To allow unlimited connection time, select Unlimited (the default).
- **Idle Timeout**—If the Inherit check box is not selected, this parameter specifies this user’s idle timeout period in minutes. If there is no communication activity on the user’s connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. The default is 30 minutes. To allow unlimited connection time, select Unlimited. This value does not apply to Clientless SSL VPN users.
- **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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring the Portal for a Group Policy

The Portal attributes determine what appears on the portal page for members of this group policy establishing Clientless SSL VPN connections. On this pane, you can enable Bookmark lists and URL Entry, file server access, Port Forwarding and Smart Tunnels, ActiveX Relay, and HTTP settings.



**Fields**

- **Bookmark List**—Select a previously-configured Bookmark list or click **Manage** to create a new one. Bookmarks appear as links, from which users can navigate from the portal page.
- **URL Entry**—Enable to allow remote users to enter URLs directly into the portal URL field.
- **File Access Control**—Controls the visibility of “hidden shares” for Common Internet File System (CIFS) files. A hidden share is identified by a dollar sign (\$) at the end of the share name. For example, drive C is shared as C\$. With hidden shares, a shared folder is not displayed, and users are restricted from browsing or accessing these hidden resources.
  - **File Server Entry**—Enable to allow remote users to enter the name of a file server.
  - **File Server Browsing**—Enable to allow remote users to browse for available file servers.
  - **Hidden Share Access**—Enable to hide shared folders.
- **Port Forwarding Control**—Provides users access to TCP-based applications over a Clientless SSL VPN connection through a Java Applet.
  - **Port Forwarding List**—Select a previously-configured list TCP applications to associate with this group policy. Click **Manage** to create a new list or to edit an existing list.
  - **Auto Applet Download**—Enables automatic installation and starting of the Applet the first time the user logs in.
  - **Applet Name**—Changes the name of the title bar that of the Applet window to the name you designate. By default, the name is Application Access.
- **Smart Tunnel**—Connects a Winsock 2, TCP-based application installed on the end station to a server on the intranet, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server.
  - **Smart Tunnel List**—Select the list name from the drop-down menu if you want to provide smart tunnel access. Assigning a smart tunnel list to a group policy or username enables smart tunnel access for all users whose sessions are associated with the group policy or username, but restricts smart tunnel access to the applications specified in the list. To view, add, modify, or delete a smart tunnel list, click the adjacent **Manage** button.
  - **Auto Start (Smart Tunnel List)**—Check to start smart tunnel access automatically upon user login. Uncheck to enable smart tunnel access upon user login, but require the user to start it manually, using the Application Access > Start Smart Tunnels button on the Clientless SSL VPN Portal Page.
  - **Auto Sign-on Server List**—Select the list name from the drop-down menu if you want to reissue the user credentials when the user establishes a smart tunnel connection to a server. Each smart tunnel auto sign-on list entry identifies a server with which to automate the submission of user credentials. To view, add, modify, or delete a smart tunnel auto sign-on list, click the adjacent **Manage** button.
  - **Domain Name (Optional)**—Specify the Windows domain to add it to the username during auto sign-on, if the universal naming convention (domain\username) is required for authentication. For example, enter CISCO to specify CISCO\jsmith when authenticating for the username jsmith. You must also check the “Use Windows domain name with user name” option when configuring associated entries in the auto sign-on server list.
- **ActiveX Relay**—Lets Clientless users launch Microsoft Office applications from the browser. The applications use the session to download and upload Microsoft Office documents. The ActiveX relay remains in force until the Clientless SSL VPN session closes.

More Options:

- **HTTP Proxy**—Enables or disables 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.
- **Auto Start (HTTP Proxy)**—Check to enable HTTP Proxy automatically upon user login. Uncheck to enable smart tunnel access upon user login, but require the user to start it manually.
- **HTTP Compression**—Enables compression of HTTP data over the Clientless SSL VPN session.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Customization for a Group Policy

To configure customization for a group policy, select a preconfigured portal customization object, or accept the customization provided in the default group policy. You can also configure a URL to display

### Fields

**Portal Customization**—Configure a customization object for the end user portal.

- **Inherit**—To inherit a portal customization from the default group policy, click **Inherit**. To specify a previously configured customization object, deselect Inherit and choose the customization object from the drop-down list.
- **Manage**—Click to import a new customization object.

**Homepage URL (optional)**— To specify a homepage URL for users associated with the group policy, enter it in this field. To inherit a home page from the default group policy, click **Inherit**.

**Access Deny Message**—To create a message to users for whom access is denied, enter it in this field. To accept the message in the default group policy, click **Inherit**.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Adding or Editing a Site-to-Site Internal Group Policy

The Add or Edit Group Policy window lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields on this window, 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 on this dialog box.

### Fields

The following attributes appear in the Add Internal Group Policy > General window. They apply to SSL VPN and IPSec sessions, or clientless SSL VPN 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 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 a security appliance; 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.
  - **IPSec**—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 client-to-LAN connections can use IPSec.
  - **L2TP/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.



**Note** If you do not select a protocol, an error message appears.

- **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 security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Group Policy window.
- **Manage**—Displays the ACL Manager window, with which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs). For more information about the ACL Manager, see the online Help for that window.

## Browse Time Range

Use the Browse Time Range dialog box to add, edit, or delete a time range. A time range is a reusable component that defines starting and ending times that can be applied to a group policy. After defining a time range, you can select the time range and apply it to different options that require scheduling. For

example, you can attach an access list to a time range to restrict access to the security appliance. A time range consists of a start time, an end time, and optional recurring (that is, periodic) entries. For more information about time ranges, see the online Help for the Add or Edit Time Range dialog box.

### Fields

- Add—Opens the Add Time Range dialog box, on which you can create a new time range.



**Note** Creating a time range does not restrict access to the device.

- Edit—Opens the Edit Time Range dialog box, on which you can modify an existing time range. This button is active only when you have selected an existing time range from the Browse Time Range table.
- Delete—Removes a selected time range from the Browse Time Range table. There is no confirmation or undo of this action.
- Name—Specifies the name of the time range.
- Start Time—Specifies when the time range begins.
- End Time—Specifies when the time range ends.
- Recurring Entries—Specifies further constraints of active time of the range within the start and stop time specified.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Time Range

The Add or Edit Time Range dialog box lets you configure a new time range.

### Fields

- Time Range Name—Specifies the name that you want to assign to this time range.
- Start Time—Defines the time when you want the time range to start.
  - Start now—Specifies that the time range starts immediately.
  - Start at—Selects the month, day, year, hour, and minute at which you want the time range to start.
- End Time—Defines the time when you want the time range to end.
  - Never end—Specifies that the time range has no defined end point.
  - End at (inclusive)—Selects the month, day, year, hour, and minute at which you want the time range to end.

- **Recurring Time Ranges**—Constrains the active time of this time range within the start and end times when the time range is active. For example, if the start time is start now and the end time is never end, and you want the time range to be effective every weekday, Monday through Friday, from 8:00 AM to 5:00 PM, you could configure a recurring time range, specifying that it is to be active weekdays from 08:00 through 17:00, inclusive.
- **Add**—Opens the Add Recurring Time Range dialog box, on which you can configure a recurring time range.
- **Edit**—Opens the Edit Recurring Time Range dialog box, on which you can modify a selected recurring time range.
- **Delete**—Removes a selected recurring time range.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## Add/Edit Recurring Time Range

The Add or Edit Recurring Time Range dialog box lets you configure or modify a recurring time range.

### Fields

- **Specify days of the week and times on which this recurring range will be active**—Makes available the options in the Days of the week area. For example, use this option when you want the time range to be active only every Monday through Thursday, from 08:00 through 16:59.
  - **Days of the week**—Select the days that you want to include in this recurring time range. Possible options are: Every day, Weekdays, Weekends, and On these days of the week. For the last of these, you can select a check box for each day that you want included in the range.
  - **Daily Start Time**—Specifies the hour and minute, in 24-hour format, when you want the recurring time range to be active on each selected day.
  - **Daily End Time (inclusive)**—Specifies the hour and minute, in 24-hour format, when you want the recurring time range to end on each selected day.
- **Specify a weekly interval when this recurring range will be active**—Makes available the options in the Weekly Interval area. The range extends inclusively through the end time. All times in this area are in 24-hour format. For example, use this option when you want the time range to be active continuously from Monday at 8:00 AM through Friday at 4:30 PM.
  - **From**—Selects the day, hour, and minute when you want the weekly time range to start.
  - **Through**—Selects the day, hour, and minute when you want the weekly time range to end.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | •        | —      |

## ACL Manager

The ACL Manager dialog box lets you define access control lists (ACLs) to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers.

- If you do not define any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic.

## Standard ACL

This pane provides summary information about standard ACLs, and lets you add or edit ACLs and ACEs.

### Fields

- Add—Lets you add a new ACL. When you highlight an existing ACL, it lets you add a new ACE for that ACL.
- Edit—Opens the Edit ACE dialog box, on which you can change an existing access control list rule.
- Delete—Removes an ACL or ACE. There is no confirmation or undo.
- Move Up/Move Down—Changes the position of a rule in the ACL Manager table.
- Cut—Removes the selection from the ACL Manager table and places it on the clipboard.
- Copy—Places a copy of the selection on the clipboard.
- Paste—Opens the Paste ACE dialog box, on which you can create a new ACL rule from an existing rule.
- No—Indicates the order of evaluation for the rule. Implicit rules are not numbered, but are represented by a hyphen.
- Address—Displays the IP address or URL of the application or service to which the ACE applies.
- Action—Specifies whether this filter permits or denies traffic flow.
- Description—Shows the description you typed when you added the rule. An implicit rule includes the following description: “Implicit outbound rule.”

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Extended ACL

This pane provides summary information about extended ACLs, and lets you add or edit ACLs and ACEs.

### Fields

- **Add**—Lets you add a new ACL. When you highlight an existing ACL, it lets you add a new ACE for that ACL.
- **Edit**—Opens the Edit ACE dialog box, on which you can change an existing access control list rule.
- **Delete**—Removes an ACL or ACE. There is no confirmation or undo.
- **Move Up/Move Down**—Changes the position of a rule in the ACL Manager table.
- **Cut**—Removes the selection from the ACL Manager table and places it on the clipboard.
- **Copy**—Places a copy of the selection on the clipboard.
- **Paste**—Opens the Paste ACE dialog box, on which you can create a new ACL rule from an existing rule.
- **No**—Indicates the order of evaluation for the rule. Implicit rules are not numbered, but are represented by a hyphen.
- **Enabled**—Enables or disables a rule. Implicit rules cannot be disabled.
- **Source**—Specifies the IP addresses (Host/Network) that are permitted or denied to send traffic to the IP addresses listed in the Destination column. In detail mode (see the Show Detail radio button), an address column might contain an interface name with the word any, such as inside: any. This means that any host on the inside interface is affected by the rule.
- **Destination**—Specifies the IP addresses (Host/Network) that are permitted or denied to send traffic to the IP addresses listed in the Source column. An address column might contain an interface name with the word any, such as outside: any. This means that any host on the outside interface is affected by the rule. An address column might also contain IP addresses; 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 firewall maps the address of the inside host to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. The address mapping structure is called an xlate, and remains in memory for a period of time. During this time, outside hosts can initiate connections to the inside host using the translated address from the pool, if allowed by the ACL. Normally, outside-to-inside connections require a static translation so that the inside host always uses the same IP address.
- **Service**—Names the service and protocol specified by the rule.
- **Action**—Specifies whether this filter permits or denies traffic flow.
- **Logging**—Shows the logging level and the interval in seconds between log messages (if you enable logging for the ACL). To set logging options, including enabling and disabling logging, right-click this column, and choose Edit Log Option. The Log Options window appears.

- **Time**—Specifies the name of the time range to be applied in this rule.
- **Description**—Shows the description you typed when you added the rule. An implicit rule includes the following description: “Implicit outbound rule.”

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit/Paste ACE

The Add/Edit/Paste ACE dialog box lets you create a new extended access list rule, or modify an existing rule. The Paste option becomes available only when you cut or copy a rule.

### Fields

- **Action**—Determines the action type of the new rule. Select either permit or deny.
  - **Permit**—Permits all matching traffic.
  - **Deny**—Denies all matching traffic.
- **Source/Destination**—Specifies the source or destination type and, depending on that type, the other relevant parameters describing the source or destination host/network IP Address. Possible values are: any, IP address, Network Object Group, and Interface IP. The availability of subsequent fields depends upon the value of the Type field:
  - **any**—Specifies that the source or destination host/network can be any type. For this value of the Type field, there are no additional fields in the Source or Destination area.
  - **IP Address**—Specifies the source or destination host or network IP address. With this selection, the IP Address, ellipsis button, and Netmask fields become available. Select an IP address or host name from the drop-down list in the IP Address field or click the ellipsis (...) button to browse for an IP address or name. Select a network mask from the drop-down list.
  - **Network Object Group**—Specifies the name of the network object group. Select a name from the drop-down list or click the ellipsis (...) button to browse for a network object group name.
  - **Interface IP**—Specifies the interface on which the host or network resides. Select an interface from the drop-down list. The default values are inside and outside. There is no browse function.
- **Protocol and Service**—Specifies the protocol and service to which this ACE filter applies. Service groups let you identify multiple non-contiguous port numbers that you want the ACL to match. For example, if you want to filter HTTP, FTP, and port numbers 5, 8, and 9, define a service group that includes all these ports. Without service groups, you would have to create a separate rule for each port.

You can create service groups for TCP, UDP, TCP-UDP, ICMP, and other protocols. A service group with the TCP-UDP protocol contains services, ports, and ranges that might use either the TCP or UDP protocol.



- Protocol—Selects the protocol to which this rule applies. Possible values are ip, tcp, udp, icmp, and other. The remaining available fields in the Protocol and Service area depend upon the protocol you select. The next few bullets describe the consequences of each of these selections:
- Protocol: TCP and UDP—Selects the TCP/UDP protocol for the rule. The Source Port and Destination Port areas allow you to specify the ports that the ACL uses to match packets.
- Source Port/Destination Port—(*Available only for TCP and UDP protocols*) Specifies an operator and a port number, a range of ports, or a well-known service name from a list of services, such as HTTP or FTP. The operator list specifies how the ACL matches the port. Choose one of the following operators: = (equals the port number), not = (does not equal the port number), > (greater than the port number), < (less than the port number), range (equal to one of the port numbers in the range).
- Group—(*Available only for TCP and UDP protocols*) Selects a source port service group. The Browse (...) button opens the Browse Source Port or Browse Destination Port dialog box.
- Protocol: ICMP—Lets you select an ICMP type or ICMP group from a preconfigured list or browse (...) for an ICMP group. The Browse button opens the Browse ICMP dialog box.
- Protocol: IP—Specifies the IP protocol for the rule in the IP protocol box. No other fields are available when you make this selection.
- Protocol: Other—Lets you select a protocol from a drop-down list, select a protocol group from a drop-down list, or browse for a protocol group. The Browse (...) button opens the Browse Other dialog box.
- Rule Flow Diagram—(*Display only*) Provides a graphical representation of the configured rule flow. This same diagram appears on the ACL Manager dialog box unless you explicitly close that display.
- Options—Sets optional features for this rule, including logging parameters, time ranges, and description.
  - Logging—Enables or disables logging or specifies the use of the default logging settings. If logging is enabled, the Syslog Level and Log Interval fields become available.
  - Syslog Level—Selects the level of logging activity. The default is Informational.
  - Log Interval—Specifies the interval for permit and deny logging. The default is 300 seconds. The range is 1 through 6000 seconds.
  - Time Range—Selects the name of the time range to use with this rule. The default is (any). Click the Browse (...) button to open the Browse Time Range dialog box to select or add a time range.
  - Description—(*Optional*) Provides a brief description of this rule. A description line can be up to 100 characters long, but you can break a description into multiple lines.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Browse Source/Destination Address

The Browse Source or Destination Address dialog box lets you select an object to use as a source or destination for this rule.

### Fields

- **Type**—Determines the type of object to use as the source or destination for this rule. Selections are IP Address Objects, IP Names, Network Object Groups, and All. The contents of the table following this field change, depending upon your selection.
- **Source/Destination Object Table**—Displays the objects from which you can select a source or destination object. If you select All in the type field, each category of object appears under its own heading. The table has the following headings:
  - **Name**—Displays the network name (which may be an IP address) for each object.
  - **IP address**—Displays the IP address of each object.
  - **Netmask**—Displays the network mask to use with each object.
  - **Description**—Displays the description entered in the Add/Edit/Paste Extended Access List Rule dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Browse Source/Destination Port

The Browse Source or Destination Port dialog box lets you select a source or destination port for this protocol in this rule.

### Fields

- **Add**—Opens the Add TCP Service Group dialog box, on which you can configure a new TCP service group.
- **Find**—Opens the Filter field.
- **Filter/Clear**—Specifies a filter criterion that you can use to search for items in the Name list, thus displaying only those items that match that criterion. When you make an entry in the Filter field, the Filter button becomes active. Clicking the Filter button performs the search. After you perform the search, the Filter button is dimmed, and the Clear button becomes active. Clicking the Clear button clears the filter field and dims the Clear button.
- **Type**—Determines the type of object to use as the source or destination for this rule. Selections are IP Address Objects, IP Names, Network Object Groups, and All. The contents of the table following this field change, depending upon your selection.
- **Name**—Lists the predefined protocols and service groups for your selection.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**Add TCP Service Group**

The Add TCP Service Group dialog box lets you configure a new a TCP service group or port to add to the browsable source or destination port list for this protocol in this rule. Selecting a member of either the Members not in Group or the Members in Group list activates the Add and Remove buttons.

**Fields**

- Group Name—Specifies the name of the new TCP service group.
- Description—(Optional) Provides a brief description of this group.
- Members not in Group—Presents the option to select either a service/service group or a port number to add to the Members in Group list.
- Service/Service Group—Selects the option to select the name of a TCP service or service group to add to the Members in Group list.
- Port #—Selects the option to specify a range of port numbers to add to the Members in Group list.
- Add—Moves a selected item from the Members not in Group list to the Members in Group list.
- Remove—Moves a selected item from the Members in Group list to the Members not in Group list.
- Members in Group—Lists the members already configured in this service group.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**Browse ICMP**

The Browse ICMP dialog box lets you select an ICMP group for this rule.

**Fields**

- Add—Opens the Add ICMP Group dialog box, on which you can configure a new TCP service group.
- Find—Opens the Filter field.

- **Filter/Clear**—Specifies a filter criterion that you can use to search for items in the Name list, thus displaying only those items that match that criterion. When you make an entry in the Filter field, the Filter button becomes active. Clicking the Filter button performs the search. After you perform the search, the Filter button is dimmed, and the Clear button becomes active. Clicking the Clear button clears the filter field and dims the Clear button.
- **Type**—Determines the type of object to use as the ICMP group for this rule. Selections are IP Address Objects, IP Names, Network Object Groups, and All. The contents of the table following this field change, depending upon your selection.
- **Name**—Lists the predefined ICMP groups for your selection.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add ICMP Group

The Add ICMP Group dialog box lets you configure a new a ICMP group by name or by number to add to the browsable ICMP list for this protocol in this rule. Selecting a member of either the Members not in Group or the Members in Group list activates the Add and Remove buttons.

#### Fields

- **Group Name**—Specifies the name of the new TCP service group.
- **Description**—(Optional) Provides a brief description of this group.
- **Members not in Group**—Presents the option to select either an ICMP type/ICMP group or an ICMP number to add to the Members in Group list.
- **ICMP Type/ICMP Group**—Selects the option to select the name of an ICMP group to add to the Members in Group list.
- **ICMP #**—Selects the option to specify an ICMP member by number to add to the Members in Group list.
- **Add**—Moves a selected item from the Members not in Group list to the Members in Group list.
- **Remove**—Moves a selected item from the Members in Group list to the Members not in Group list.
- **Members in Group**—Lists the members already configured in this service group.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Browse Other

The Browse Other dialog box lets you select a protocol group for this rule.

### Fields

- **Add**—Opens the Add Protocol Group dialog box, on which you can configure a new service group.
- **Find**—Opens the Filter field.
- **Filter/Clear**—Specifies a filter criterion that you can use to search for items in the Name list, thus displaying only those items that match that criterion. When you make an entry in the Filter field, the Filter button becomes active. Clicking the Filter button performs the search. After you perform the search, the Filter button is dimmed, and the Clear button becomes active. Clicking the Clear button clears the filter field and dims the Clear button.
- **Type**—Determines the type of object to use as the protocol group for this rule. Selections are IP Address Objects, IP Names, Network Object Groups, and All. The contents of the table following this field change, depending upon your selection.
- **Name**—Lists the predefined protocol groups for your selection.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add Protocol Group

The Add Protocol Group dialog box lets you configure a new a protocol group by name or by number to add to the browsable protocol list for this rule. Selecting a member of either the Members not in Group or the Members in Group list activates the Add and Remove buttons.

### Fields

- **Group Name**—Specifies the name of the new TCP service group.
- **Description**—(Optional) Provides a brief description of this group.
- **Members not in Group**—Presents the option to select either a protocol/protocol group or a protocol number to add to the Members in Group list.
- **Protocol/Protocol Group**—Selects the option to select the name of a protocol or protocol group to add to the Members in Group list.
- **Protocol #**—Selects the option to specify a protocol by number to add to the Members in Group list.
- **Add**—Moves a selected item from the Members not in Group list to the Members in Group list.
- **Remove**—Moves a selected item from the Members in Group list to the Members not in Group list.
- **Members in Group**—Lists the members already configured in this service group.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Servers

The Add or Edit Group Policy window, Servers item lets you specify DNS and WINS servers, as well as the DHCP scope and default domain.

## Add/Edit Internal Group Policy > IPSec Client

The 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.

### Fields

- Re-Authentication on IKE Re-key—Enables or disables reauthentication when IKE re-key occurs, unless the Inherit check box is selected. 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.
- Enable extended reauth-on-rekey to allow entry of authentication credentials until SA expiry—Allow 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 selected.
- 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—Enables locking the tunnel group you select from the list, 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Client Access Rules

The table on this dialog box lets you view up to 25 client access rules. If you deselect the Inherit check box, the Add, Edit, and Delete buttons become active and the following column headings appear in the table:

- Priority—Shows the priority for this rule.
- Action—Specifies whether this rule permits or denies access.
- Client Type—Specifies the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset.
- VPN Client Version—Specifies the version or versions of the VPN client to which this rule applies. This box contains a comma-separated list of software or firmware images appropriate for this client.

### Modes

The following table shows the modes in which this feature is available:

## Add/Edit Client Access Rule

The Add or Edit Client Access Rule dialog box adds a new client access rule for an IPSec group policy or modifies an existing rule.

### Fields

- Priority—Shows the priority for this rule.
- Action—Specifies whether this rule permits or denies access.
- VPN Client Type—Specifies the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset. Some common values for VPN Client Type include VPN 3002, PIX, Linux, \* (matches all client types), Win9x (matches Windows 95, Windows 98, and Windows ME), and WinNT (matches Windows NT, Windows 2000, and Windows XP). If you choose \*, do not configure individual Windows types such as Windows NT.
- VPN Client Version—Specifies the version or versions of the VPN client to which this rule applies. This box contains a comma-separated list of software or firmware images appropriate for this client. The following caveats apply:

- You must specify the software version for this client. You can specify \* to match any version.
- Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the VPN 3002.
- The TFTP server for distributing the hardware client image must be a robust TFTP server.
- If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order.
- A VPN client user must download an appropriate software version from the listed URL.
- The VPN 3002 hardware client software is automatically updated via TFTP.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Client Configuration Tab

The Add or Edit Group Policy window, Client Configuration tab contains three tabs that let you configure general client parameters, Cisco client parameters, and Microsoft client parameters.

For information about the individual tabs, see the following links:

- [Add/Edit Internal Group Policy > Client Configuration Tab > General Client Parameters Tab](#)
- [Add/Edit Internal Group Policy > Client Configuration Tab > Cisco Client Parameters Tab](#)
- [Add or Edit Internal Group Policy > Advanced > IE Browser Proxy](#)

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Client Configuration Tab > General Client Parameters Tab

This tab configures client attributes that are common across both Cisco and Microsoft clients, including the banner text, default domain, split tunnel parameters, and address pools.



### Note

The AnyConnect VPN Client and the SSL VPN Client do not support split DNS.



### Fields

- **Inherit**—(Multiple instances) Indicates that the corresponding setting takes its value from the default group policy. Deselecting the Inherit check box makes other options available for the parameter. This is the default option for all attributes on this tab.
- **Banner**—Specifies whether to inherit the banner from the default group policy or enter new banner text. For more information, see [View/Config Banner](#)
- **Edit Banner**—Displays the View/Config Banner dialog box, in which you can enter banner text, up to 500 characters.
- **Default Domain**—Specifies whether to inherit the default domain from the default group policy or use a new default domain specified in the field.
- **Split Tunnel DNS Names (space delimited)**—Specifies whether to inherit the split-tunnel DNS names or from the default group policy or specify a new name or list of names in the field.
- **Split Tunnel Policy**—Specifies whether to inherit the split-tunnel policy from the default group policy or select a policy from the menu. The menu options are to tunnel all networks, tunnel those in the network list below, or exclude those in the network list below.
- **Split Tunnel Network List**—Specifies whether to inherit the split-tunnel network list from the default group policy or select from the drop-down list.
- **Manage**—Opens the ACL Manager dialog box, on which you can manage standard and extended access control lists.
- **Address Pools**—Configures the address pools available through this group policy.
  - **Available Pools**—Specifies a list of address pools for allocating addresses to remote clients. Deselecting the Inherit check box with no address pools in the Assigned Pools list indicates that no address pools are configured and disables inheritance from other sources of group policy.
  - **Add**—Moves the name of an address pool from the Available Pools list to the Assigned Pools list.
  - **Remove**—Moves the name of an address pool from the Assigned Pools list to the Available Pools list.
  - **Assigned Pools (up to 6 entries)**—Lists the address pools you have added to the assigned pools list. The address-pools settings in this table override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation. The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## View/Config Banner

The View/Config Banner dialog box lets you enter into the text box up to 500 characters of text to be displayed as a banner for the specified client.

**Note**

A carriage return/line feed, created by pressing Enter, counts as 2 characters.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Client Configuration Tab > Cisco Client Parameters Tab

This tab configures client attributes that are specific to Cisco clients, including password storage, enabling or disabling IPSec over UDP and setting the UDP port number, and configuring IPSec backup servers.

**Fields**

- 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.
- 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.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add or Edit Internal Group Policy > Advanced > IE Browser Proxy

This dialog box configures attributes for Microsoft Internet Explorer.

### Fields

- 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. Select 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 box in the Proxy Settings dialog box in Internet Explorer.
- 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. For details about .pac files, see the following Microsoft Knowledge Base article:

<http://www.microsoft.com/mind/0599/faq/faq0599.asp>.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Standard Access List Rule

The Add/Edit Standard Access List Rule dialog box lets you create a new rule, or modify an existing rule.

### Fields

- Action—Determines the action type of the new rule. Select either permit or deny.
  - Permit—Permits all matching traffic.
  - Deny—Denies all matching traffic.
- Host/Network IP Address—Identifies the networks by IP address.
  - IP address—The IP address of the host or network.
  - Mask—The subnet mask of the host or network
- Description—(Optional) Enter a description of the access rule.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Client Firewall Tab

The Add or Edit Group Policy window, Client Firewall tab, lets you configure firewall settings for VPN clients for the group policy being added or modified.

**Note**

Only VPN clients running Microsoft Windows can use these firewall features. They are currently not available to hardware clients or other (non-Windows) software clients.

A *firewall* isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN. Remote users connecting to the security appliance 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 security appliance. (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 security appliance.) 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 security appliance, 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 security appliance pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

**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 tab and 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 select No Firewall (the default), none of the remaining fields on this window are active. If you want users in this group to be firewall-protected, select either the Firewall Required or Firewall Optional setting.

If you select Firewall Required, all users in this group must use the designated firewall. The security appliance drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the security appliance 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 and VPN 3002 hardware clients) 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 select 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 security appliance 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 select this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active. The security appliance 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 menu. The choices available on the menu are filters defined on this security appliance, including the default filters. Keep in mind that the security appliance pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the security appliance. 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 security appliance 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 window, on which you can configure Access Control Lists (ACLs).

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Internal Group Policy > Hardware Client Tab

The Add or Edit Group Policy > Hardware Client dialog box lets you configure settings for the VPN 3002 hardware client for the group policy being added or modified. The Hardware Client tab parameters do not pertain to the ASA 5505 in client mode.

### Fields

- **Inherit**—(Multiple instances) Indicates that the corresponding setting takes its value from the default group policy, rather than from the explicit specifications that follow. This is the default setting for all attributes in this tab.
- **Require Interactive Client Authentication**—Enables or disables the requirement for interactive client authentication. This parameter is disabled by default. Interactive hardware client authentication provides additional security by requiring the VPN 3002 to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled, the VPN 3002 does not have a saved username and password. When you enter the username and password, the VPN 3002 sends these credentials to the security appliance to which it connects. The security appliance facilitates authentication, on either the internal or an external authentication server. If the username and password are valid, the tunnel is established.

When you enable interactive hardware client authentication for a group, the security appliance pushes that policy to the VPN 3002s in the group. If you have previously set a username and password on the VPN 3002, the software deletes them from the configuration file. When you try to connect, the software prompts you for a username and password.

If, on the security appliance, you subsequently disable interactive hardware authentication for the group, it is enabled locally on the VPN 3002s, and the software continues to prompt for a username and password. This lets the VPN 3002 connect, even though it lacks a saved username and password, and the security appliance has disabled interactive hardware client authentication. If you subsequently configure a username and password, the feature is disabled, and the prompt no longer appears. The VPN 3002 connects to the security appliance using the saved username and password.

- **Require Individual User Authentication**—Enables or disables the requirement for individual user authentication for users behind ASA 5505 in client mode or the VPN 3002 hardware client in the group. To display a banner to hardware clients in a group, individual user authentication must be enabled. This parameter is disabled by default.

Individual user authentication protects the central site from access by unauthorized persons on the private network of the hardware client. When you enable individual user authentication, each user that connects through a hardware client must open a web browser and manually enter a valid username and password to access the network behind the security appliance, even though the tunnel already exists.



### Note

You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

If you have a default home page on the remote network behind the security appliance, or if you direct the browser to a website on the remote network behind the security appliance, the hardware client directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.

If you try to access resources on the network behind the security appliance that are not web-based, for example, e-mail, the connection fails until you authenticate using a browser.

To authenticate, you must enter the IP address for the private interface of the hardware client in the browser Location or Address field. The browser then displays the login screen for the hardware client. To authenticate, click the Connect/Login Status button.

One user can log in for a maximum of four sessions simultaneously. Individual users authenticate according to the order of authentication servers configured for a group.

- **User Authentication Idle Timeout**—Configures a user timeout period. The security appliance terminates the connection if it does not receive user traffic during this period. You can specify that the timeout period is a specific number of minutes or unlimited.
  - **Unlimited**—Specifies that the connection never times out. This option prevents inheriting a value from a default or specified group policy.
  - **Minutes**—Specifies the timeout period in minutes. Use an integer between 1 and 35791394. The default value is Unlimited.

Note that the idle timeout indicated in response to the `show uauth` command is always the idle timeout value of the user who authenticated the tunnel on the Cisco Easy VPN remote device.

- **Cisco IP Phone Bypass**—Lets Cisco IP phones bypass the interactive individual user authentication processes. If enabled, interactive hardware client authentication remains in effect. Cisco IP Phone Bypass is disabled by default.



---

**Note** You must configure the ASA 5505 in client mode or the VPN 3002 hardware client to use network extension mode for IP phone connections.

---

- **LEAP Bypass**—Lets LEAP packets from Cisco wireless devices bypass the individual user authentication processes (if enabled). LEAP Bypass lets LEAP packets from devices behind a hardware client travel across a VPN tunnel *prior* to individual user authentication. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per individual user authentication (if enabled). LEAP Bypass is disabled by default.



---

**Note** This feature does not work as intended if you enable interactive hardware client authentication.

---

IEEE 802.1X is a standard for authentication on wired and wireless networks. It provides wireless LANs with strong mutual authentication between clients and authentication servers, which can provide dynamic per-user, per-session wireless encryption privacy (WEP) keys, removing administrative burdens and security issues that are present with static WEP keys.

Cisco Systems has developed an 802.1X wireless authentication type called Cisco LEAP. LEAP implements mutual authentication between a wireless client on one side of a connection and a RADIUS server on the other side. The credentials used for authentication, including a password, are always encrypted before they are transmitted over the wireless medium.



**Note**

Cisco LEAP authenticates wireless clients to RADIUS servers. It does not include RADIUS accounting services.

LEAP users behind a hardware client have a circular dilemma: they cannot negotiate LEAP authentication because they cannot send their credentials to the RADIUS server behind the central site device over the tunnel. The reason they cannot send their credentials over the tunnel is that they have not authenticated on the wireless network. To solve this problem, LEAP Bypass lets LEAP packets, and only LEAP packets, traverse the tunnel to authenticate the wireless connection to a RADIUS server before individual users authenticate. Then the users proceed with individual user authentication.

LEAP Bypass works as intended under the following conditions:

- The interactive unit authentication feature (intended for wired devices) must be disabled. If interactive unit authentication is enabled, a non-LEAP (wired) device must authenticate the hardware client before LEAP devices can connect using that tunnel.
- Individual user authentication is enabled (if it is not, you do not need LEAP Bypass).
- Access points in the wireless environment must be Cisco Aironet Access Points. The wireless NIC cards for PCs can be other brands.
- The Cisco Aironet Access Point must be running Cisco Discovery Protocol (CDP).
- The ASA 5505 or VPN 3002 can operate in either client mode or network extension mode.
- LEAP packets travel over the tunnel to a RADIUS server via ports 1645 or 1812.

**Note**

Allowing any unauthenticated traffic to traverse the tunnel might pose a security risk.

- Allow Network Extension Mode—Restricts the use of network extension mode on the hardware client. Select the option to let hardware clients use network extension mode. Network extension mode is required for the hardware client to support IP phone connections, because the Call Manager can communicate only with actual IP addresses.

**Note**

If you disable network extension mode, the default setting, the hardware client can connect to this security appliance in PAT mode only. If you disallow network extension mode here, be careful to configure all hardware clients in a group for PAT mode. If a hardware client is configured to use network extension mode and the security appliance to which it connects disables network extension mode, the hardware client attempts to connect every 4 seconds, and every attempt is rejected. In this situation, the hardware client puts an unnecessary processing load on the security appliance to which it connects; large numbers of hardware clients that are misconfigured in this way reduces the ability of the security appliance to provide service.

**Modes**

The following table shows the modes in which this feature is available:

## Add/Edit Server and URL List

The Add or Edit Server and URL List dialog box lets you add, edit, delete, and order the items in the designated URL list.

**Fields**

- List Name—Specifies the name of the list to be added or selects the name of the list to be modified or deleted.
- URL Display Name—Specifies the URL name displayed to the user.
- URL—Specifies the actual URL associated with the display name.
- Add—Opens the Add Server or URL dialog box, on which you can configure a new server or URL and display name.
- Edit—Opens the Edit Server or URL dialog box, on which you can configure a new server or URL and display name.
- Delete—Removes the selected item from the server and URL list. There is no confirmation or undo.
- Move Up/Move Down—Changes the position of the selected item in the server and URL list.

**Add/Edit Server or URL**

The Add or Edit Server or URL dialog box lets you add or edit, delete, and order the items in the designated URL list.

**Fields**

- URL Display Name—Specifies the URL name displayed to the user.
- URL—Specifies the actual URL associated with the display name.

## Configuring SSL VPN Connections

Use this window and its child windows to specify SSL VPN connection attributes for client-based connections. These attributes apply to the Cisco AnyConnect VPN Client and to the legacy SSL VPN Client.

On the main window, you can enable client access on the interfaces you select and you can select, add, edit, and delete connections (tunnel groups). You can also specify whether you want to allow a user to select a particular connection at login.

**Fields**

Access Interfaces—Specify SSL VPN client access for each interface listed in the table:

- Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces in the table below—Enables access on the interfaces that have “Allow Access” checked.
- Interface—The interface to enable SSL VPN Client connections.
- Allow Access—Check to allow access.
- Require Client Certificate—Check to require a valid certificate from the client before allowing connection.
- Enable DTLS—Check to enable Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- Access Port—Specify the port for SSL VPN Client connections.
- DTLS Port—Specify the port for DTLS connections.

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 select 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.

## Setting the Basic Attributes for an SSL VPN Connection

To set the basic attributes for an SSL VPN connection, choose Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connections > Add or Edit > Basic. The Add SSL VPN Connection (Basic) window opens.

### Fields

Set the attributes in the Add SSL VPN Connection (Basic) window as follows:

- Aliases—(Optional) Enter one or more alternative names for the connection. You can spaces or punctuation to separate the names.
- Authentication—Choose one of the following methods to use to authenticate the connection: AAA, Certificate, or Both.
- AAA Server Group—Choose a AAA server group from the drop-down list. The default setting is LOCAL, which specifies that the security appliance handles the authentication. Before making a selection, you can click **Manage** to open a dialog box over this window to view or make changes to the security appliance configuration of AAA server groups.

Selecting something other than LOCAL makes available the Use LOCAL if Server Group Fails check box.

- Use LOCAL if Server Group fails—Check to enable or uncheck to disable the LOCAL database if the group specified by the Authentication Server Group attribute fails.
- DHCP Servers—Enter the name or IP address of a DHCP server to use.
- Client Address Pools—Enter the pool name of an available, configured pool of IP addresses to use for client address assignment. Before making a selection, you can click **Select** to open a dialog box over this window to view or make changes to the address pools.
- 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.
- SSL VPN Client Protocol—Check Enabled to enable SSL VPN for uncheck to disable it.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Setting Advanced Attributes for an IPsec or SSL VPN Connection

Use the advanced attributes to fine-tune the parameters of the IPsec or SSL VPN connection.

## Setting General Attributes for an IPsec or SSL VPN Connection

Choose Advanced > General in the Add IPsec Remote Access Connection or Add SSL VPN Connection to specify whether to strip the realm and group from the username before passing them to the AAA server, and to set the password management parameters.

### Fields

Set the attributes in this window Add IPsec Remote Access Connection or Add SSL VPN Connection (General) window as follows:

- 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@it.cisco.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 security appliance 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@it.cisco.com#VPNGroup`. If you choose this option, you must use either the # or ! character for the group delimiter because the security appliance cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

A Kerberos realm is a special case. The convention in naming a Kerberos realm is to capitalize the DNS domain name associated with the hosts in the Kerberos realm. For example, if users are in the it.cisco.com domain, you might call your Kerberos realm IT.CISCO.COM.

- 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 Enable Group Lookup. When you append a group name to a username using a delimiter, and enable Group Lookup, the security appliance 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.

The security appliance supports password management for the RADIUS and LDAP protocols. It supports the “password-expire-in-days” option only for LDAP. This parameter is valid for AAA servers that support such notification. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

You can configure password management for IPsec remote access and SSL VPN tunnel-groups.



**Note** Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This feature requires MSCHAPv2, so please check with your vendor.

The security appliance, releases 7.1 and later, 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
- Clientless SSL VPN

Password management is *not* supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the security appliance perspective, it is talking 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 security appliance 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.

- Override account-disabled indication from AAA server—Overrides an account-disabled indication from a AAA server.



**Note** Allowing override account-disabled is a potential security risk.

- Enable notification upon password expiration to allow user to change password—Checking this attribute makes the following two parameters available. You can select 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.

In either case, and, if the password expires without being changed, the security appliance 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.

**Note**

This does not change the number of days before the password expires, but rather, it enables the notification. If you select this option, you must also specify the number of days.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring SSL VPN Client Connections

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. The client gives remote users the benefits of an SSL VPN client without the need for network administrators to install and configure clients on remote computers.

Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Release Notes*.

The security appliance downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

**Fields**

- **Inherit**—(Multiple instances) Indicates that the corresponding setting takes its value from the default group policy, rather than from the explicit specifications that follow. This is the default setting for all attributes in this pane.

- **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 Transport Layer Security (DTLS)**—DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.
- **Keepalive Messages**—Enter an 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.
- **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.
- **Client Profile to Download**—a profile is a group of configuration parameters that the AnyConnect client uses to configure the connection entries that appear in the user interface, including the names and addresses of host computers.
- **Optional Client Module to Download**—To minimize download time, the AnyConnect client only requests downloads (from the security appliance) of modules that it needs for each feature that it supports. You must specify the names of modules that enable other features, such as *sbl* to enable the feature Start Before Logon (SBL).

For a list of values to enter for each client feature, see the release notes for the Cisco AnyConnect VPN Client.

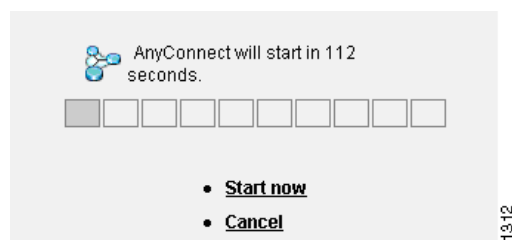
### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Login Setting

In this window, you can enable the security appliance to prompt remote users to download the AnyConnect client. [Figure 35-1](#) shows the prompt displayed:

**Figure 35-1** Prompt Displayed to Remote Users for SSL VPN Client Download**Fields**

- **Inherit**—Check to inherit the value from the default group policy.
- **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.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

**Key Regeneration**

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

**Fields**

- **Renegotiation Interval**—Clear 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**—Check the **None** check box to disable rekey, check the **SSL** check box to specify SSL renegotiation during a rekey, or check the **New Tunnel** check box to establish a new tunnel during rekey.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |



## Dead Peer Detection

Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed.

### Fields

- **Gateway Side Detection**—Uncheck the **Disable** check box to specify that DPD is performed by the security appliance (gateway). Enter the interval, from 30 to 3600 seconds, with which the security appliance performs DPD.
- **Client Side Detection**—Uncheck the **Disable** check box to specify that DPD is performed by the client. Enter the interval, from 30 to 3600 seconds, with which the client performs DPD.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Customization

### Fields

- **Portal Customization**—Selects the customization to apply to the AnyConnect Client/SSL VPN portal page. The default is DfltCustomization.
- **Manage**—Opens the Configure GUI Customization objects dialog box, on which you can specify that you want to add, edit, delete, import, or export a customization object.
- **Access Deny Message**—Specifies a message to display to the end user when the connection is denied. Select Inherit to accept the message in the default group policy. The default message, if you deselect Inherit, is: “Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.”

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## ACLs

This window lets you configure ACLs for Clientless SSL VPN.

**Fields**

- View (Unlabeled)—Indicates whether the selected entry is expanded (minus sign) or contracted (plus sign).
- # column—Specifies the ACE ID number.
- Enable—Indicates whether this ACL is enabled or disabled. You can enable or disable the ACL using this check box.
- Action—Specifies whether this ACL permits or denies access.
- Type—Specifies whether this ACL applies to a URL or a TCP address/port.
- Filter—Specifies the type of filter being applied.
- Syslog Level (Interval)—Specifies the syslog parameters for this ACL.
- Time Range—Specifies the name of the time range, if any, for this ACL. The time range can be a single interval or a series of periodic ranges.
- Description—Specifies the description, if any, of the ACL.
- Add ACL—Displays the Add Web Type ACL dialog box, in which you can specify an ACL ID.
- Add ACE—Displays the Add Web Type ACE dialog box, in which you specify parameters for the named ACL. This button is active only if there are one or more entries in the Web Type ACL table.
- Edit ACE/Delete—Click to edit or delete the highlighted ACL or ACE. When you delete an ACL, you also delete all of its ACEs. No warning or undelete.
- Move Up/Move Down—Highlight an ACL or ACE and click these buttons to change the order of ACLs and ACEs. The security appliance checks ACLs and their ACEs in priority order according to their position in the ACLs list box until it finds a match.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Clientless SSL VPN Connections

Use the Clientless SSL VPN Access Connections window to configure clientless SSL VPN access parameters. This window also records the configuration choices you make in its child dialog boxes.

**Fields**

- Access Interfaces—Lets you select from a table the interfaces on which to enable access. The fields in this table include the interface name and check boxes enabling you whether to allow access and require a certificate for authentication.
- Access Port—Specifies the access port for the connection. The default value is 443.
- Connections—Provides a connection table that shows the records that determine the connection policy for this connection (tunnel group). Each record identifies a default group policy for the connection and contains protocol-specific connection parameters.

- Add—Opens the Add Clientless SSL VPN dialog box for the selected connection.
- Edit—Opens the Edit Clientless SSL VPN dialog box for the selected connection.
- Delete—Removes the selected connection from the table. There is no confirmation or undo.
- Allow user to select connection, identified by alias in the table above, at login page—Specifies that the user login page presents the user with a drop-down menu from which the user can select a particular tunnel group with which to connect.

## Add or Edit Clientless SSL VPN Connections

The Add or Edit SSL VPN dialog box consists of Basic and Advanced sections, accessible through the expandable menu on the left of the box.

### Add or Edit Clientless SSL VPN Connections > Basic

The Basic dialog box lets you configure essential characteristics for this connection.

#### Fields

- Name—Specifies the name of the connection. For the edit function, this field is read-only.
- Aliases—(Optional) Specifies one or more alternate names for this connection. The aliases appear on the login page if you configure that option on the Clientless SSL VPN Access Connections window.
- Authentication—Specifies the authentication parameters.
  - Method—Specifies whether to use AAA authentication, certificate authentication, or both methods for this connection. The default is AAA authentication.
  - AAA server Group—Selects the AAA server group to use for authenticating this connection. The default is LOCAL.
  - Manage—Opens the Configure AAA Server Groups dialog box.
- Default Group Policy—Specifies the default group policy parameters to use for this connection.
  - Group Policy—Selects the default group policy to use for this connection. The default is DfltGrpPolicy.
  - Clientless SSL VPN Protocol—Enables or disables the Clientless SSL VPN protocol for this connection.

### Add or Edit Clientless SSL VPN Connections > Advanced

The Advanced menu items and their dialog boxes let you configure the following characteristics for this connection:

- General attributes.
- Authentication attributes.
- Authorization attributes.
- Accounting attributes.
- Name server attributes.

- Clientless SSL VPN attributes.

## Add or Edit Clientless SSL VPN Connections > Advanced > General

Use this window to specify whether to strip the realm and group from the username before passing them to the AAA server, and to specify password management options.

### Fields

- 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@it.cisco.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 security appliance 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@it.cisco.com#VPNGroup`. If you choose this option, you must use either the # or ! character for the group delimiter because the security appliance cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

A Kerberos realm is a special case. The convention in naming a Kerberos realm is to capitalize the DNS domain name associated with the hosts in the Kerberos realm. For example, if users are in the `it.cisco.com` domain, you might call your Kerberos realm `IT.CISCO.COM`.

- 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 security appliance 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.
  - Override account-disabled indication from AAA server—Overrides an account-disabled indication from a AAA server.



### Note

Allowing override account-disabled is a potential security risk.

- Enable notification upon password expiration to allow user to change password—Checking this check box makes the following two parameters available. You can select 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 select this option, you must also specify the number of days.

In either case, and, if the password expires without being changed, the security appliance 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 security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add or Edit Clientless SSL VPN Connection Profile or IPSec Connection Profiles > Advanced > Authentication

The Authentication dialog box lets you view, add, edit, or delete interface-specific authentication server groups. Each row of the table on 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.

### Fields

- **Add or Edit**—Opens the Assign Authentication Server Group to Interface dialog box, on 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.
- **Delete**—Removes the selected server group from the table. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Assign Authentication Server Group to Interface

This dialog box lets you associate an interface with a AAA server group. The results appear in the table on the Authentication dialog box.

### Fields

- Interface—Selects an interface, DMZ, Outside, or Inside. The default is DMZ.
- Server Group—Selects a server group to assign to the selected interface. The default is LOCAL.
- Manage—Opens the Configure AAA Server Groups dialog box.
- Fallback—Enables or disables fallback to LOCAL if the selected server group fails.

## Add or Edit SSL VPN Connections > Advanced > Authorization

This dialog box lets you configure the default authorization server group, interface-specific authorization server groups, and user name mapping attributes. The attributes are the same for SSL VPN and Clientless SSL VPN connections.

### Fields

- Default Authorization Server Group—Configures default authorization server group attributes.
  - Server Group—Selects the authorization server group to use for this connection. The default is --None--.
  - Manage—Opens the Configure AAA Server Groups window.
  - Users must exist in the authorization database to connect—Enables or disables this requirement.
- Interface-specific Authorization Server Groups
  - Table—Lists each configured interface and the server group with which it is associated.
  - Add or Edit—Opens the Assign Authorization Server Group to Interface window.
  - Delete—Removes the selected row from the table.
- User Name Mapping—Specifies user name mapping attributes.
  - Use the entire DN as the username—Enables or disables the requirement to use the entire DN as the username.
  - Specify individual DN fields as the username. You can select both the primary DN field, for which the default is CN (Common Name) and the secondary DN field, for which the default is OU (Organization Unit).

## Assign Authorization Server Group to Interface

This dialog box lets you associate an interface with a AAA server group. The results appear in the table on the Authorization dialog box.

### Fields

- Interface—Selects an interface, DMZ, Outside, or Inside. The default is DMZ.
- Server Group—Selects a server group to assign to the selected interface. The default is LOCAL.
- Manage—Opens the Configure AAA Server Groups dialog box.

## Add or Edit SSL VPN Connections > Advanced > SSL VPN

This dialog box lets you configure attributes that affect what the remote user sees upon login.

### Fields

- Login Page Customization—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization.
- Manage—Opens the Configure GUI Customization Objects window.
- Connection Aliases—Lists in a table the existing connection aliases and their status and lets you add or delete items in that table. A connection alias appears on the user login page if the connection is configured to allow users to select a particular connection (tunnel group) at login.
  - Add—Opens the Add Connection Alias window, on which you can add and enable a connection alias.
  - Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.
- Group URLs—Lists in a table the existing group URLs and their status and lets you add or delete items in that table. A group URL appears on the user login page if the connection is configured to allow users to select a particular group at login.
  - Add—Opens the Add Group URL window, on which you can add and enable a group URL.
  - Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.

## Add or Edit Clientless SSL VPN Connections > Advanced > SSL VPN

This dialog box lets you configure attributes that affect what the remote user sees upon login.

### Fields

- Login Page Customization—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization.
- Manage—Opens the Configure GUI Customization Objects window.
- Connection Aliases—Lists in a table the existing connection aliases and their status and lets you add or delete items in that table. A connection alias appears on the user login page if the connection is configured to allow users to select a particular connection (tunnel group) at login.
  - Add—Opens the Add Connection Alias window, on which you can add and enable a connection alias.
  - Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.
- Group URLs—Lists in a table the existing group URLs and their status and lets you add or delete items in that table. A group URL appears on the user login page if the connection is configured to allow users to select a particular group at login.
  - Add—Opens the Add Group URL window, on which you can add and enable a group URL.
  - Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.

## Add or Edit Clientless SSL VPN Connections > Advanced > Name Servers

The table on this dialog box shows the attributes of the already-configured NetBIOS servers. The Add or Edit Tunnel Group window for Clientless SSL VPN access, NetBIOS dialog box, lets you configure the NetBIOS attributes for the tunnel group. Clientless SSL VPN uses NetBIOS and the Common Internet File System protocol to access or share files on remote systems. When you attempt a file-sharing connection to a Windows computer by using its computer name, the file server you specify corresponds to a specific NetBIOS name that identifies a resource on the network.

The security appliance queries NetBIOS name servers to map NetBIOS names to IP addresses. Clientless SSL VPN requires NetBIOS to access or share files on remote systems.

To make the NBNS function operational, you must configure at least one NetBIOS server (host). You can configure up to 3 NBNS servers for redundancy. The security appliance uses the first server on the list for NetBIOS/CIFS name resolution. If the query fails, it uses the next server.

### Fields

- IP Address—Displays the IP addresses of configured NetBIOS servers.
- Master Browser—Shows whether a server is a WINS server or one that can also be a CIFS server (that is, a master browser).
- Timeout (seconds)—Displays the initial time in seconds that the server waits for a response to an NBNS query before sending the query to the next server.
- Retries—Shows the number of times to retry sending an NBNS query to the configured servers, in order. In other words, this is the number of times to cycle through the list of servers before returning an error. The minimum number of retries is 0. The default number of retries is 2. The maximum number of retries is 10.
- Add/Edit—Click to add a NetBIOS server. This opens the Add or Edit NetBIOS Server dialog box.
- Delete—Removes the highlighted NetBIOS row from the list.
- Move Up/Move Down—The security appliance sends NBNS queries to the NetBIOS servers in the order in which they appear in this box. Use this box to change the priority order of the servers by moving them up or down in the list.

### Fields

- 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 DNS Server Groups

This 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 on this dialog box.

### Fields

- Add or Edit—Opens the Add or Edit DNS Server Group dialog box..
- Delete—Removes the selected row from the table. There is no confirmation or undo.



## Add or Edit Clientless SSL VPN Connections > Advanced > Clientless SSL VPN

This dialog box lets you specify portal-related attributes for Clientless SSL VPN connections.

### Fields

- Portal Page Customization—Selects the customization to apply to the user interface.
- Manage—Opens the Configure GUI Customization Objects dialog box.

## IPSec Remote Access Connection Profiles

The parameters in the IPSec ConnectionProfiles window let you configure IPSec remote access connections. Most of the parameters in this section were formerly configured under tunnel groups. An IPSec connection represents a connection-specific record for IPSec and Clientless SSL VPN connections.

The IPSec group uses the IPSec connection parameters to create a tunnel. An IPSec connection can be either remote-access or Site-to-Site. The IPSec group is configured on the internal server or on an external RADIUS server. For ASA 5505 in client mode or VPN 3002 hardware client parameters, which enable or disable interactive hardware client authentication and individual user authentication, the IPSec connection parameters take precedence over parameters set for users and groups.

The Clientless SSL VPN tunnel-group parameters are the parameters of the Clientless SSL VPN group that you want to apply to this IPSec connection. You configure Clientless SSL VPN access on the Configuration > Clientless SSL VPN window.

### Fields

- Access Interfaces—Selects the interfaces to enable for IPSec access. The default is that no access is selected.
- Connections—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 connection.
  - ID Certificate—Specifies the name of the ID certificate, if available.
  - IPSec Protocol—Indicates whether the IPSec protocol is enabled. You enable this protocol on the Add or Edit IPSec Remote Access Connection, Basic window.
  - L2TP/IPSec Protocol—Indicates whether the L2TP/IPSec protocol is enabled. You enable this protocol on the Add or Edit IPSec Remote Access Connection, Basic window.
  - Group Policy—Indicates the name of the group policy for this IPSec connection.
- Add or Edit—Opens the Add or Edit IPSec Remote Access Connection Profile dialog box.
- Delete—Removes the selected server group from the table. There is no confirmation or undo.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add or Edit an IPSec Remote Access Connection Profile

The Add or Edit IPSec Remote Access Connection Profile dialog box has a navigation pane that lets you select basic or advanced elements to configure.

### Add or Edit IPSec Remote Access Connection Profile Basic

The Add or Edit IPSec Remote Access Connection Profile Basic dialog box lets you configure common attributes for IPSec connections.

#### Fields

- 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.
  - Identity Certificate—Selects the name of an identity certificate, if any identity certificates are configured and enrolled.
  - Manage—Opens the Manage Identity Certificates window, 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.
  - 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. To define an address pool, go to Configuration > Remote Access VPN > Network Client Access > Address Assignment > Address Pools.
  - Select—Opens the Select 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Mapping Certificates to IPSec or SSL VPN Connection Profiles

When the security appliance receives an IPSec or SSL connection request with a client certificate authentication, it evaluates the attributes of the certificate using a set of 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 the security appliance fails to find a match, it assigns the DefaultWEBVPNGroup profile to the connection and lets the user choose the connection profile from a drop-down menu displayed on the portal page, if it is enabled.

To configure the evaluation of IPSec or SSL VPN connections against certificate criteria-based rules, use the IPSec Certificate to Connection Maps > Rules or Certificate to SSL VPN Connections Profile Maps panel.

This panel lets you create the certificate-based criteria for each IPSec and SSL VPN connection profile, as follows:

- 
- Step 1** Use the table at the top (Certificate to Connection Profile Maps) to do one of the following:
- Create a list name, called a “map,” specify the priority of the list, and assign the list to a connection profile.  
ASDM highlights the list after you add it to the table.
  - Confirm that a list is assigned to the connection profile for which you want to add certificate-based rules.  
ASDM highlights the list after you add it to the table and displays any associated list entries in the table at the bottom of the pane.
- Step 2** Use the table at the bottom (Mapping Criteria) to view, add, change or delete entries to the selected list. Each entry in the list consists of one certificate-based rule. All of the rules in the mapping criteria list need to match the contents of the certificate for the security appliance to choose the associated map index. To assign a connection if one criterion or another matches, create one list for each matching criterion.
- 

To understand the fields, see the following sections:

- [Add/Edit Certificate Matching Rule](#)

- [Add/Edit Certificate Matching Rule Criterion](#)

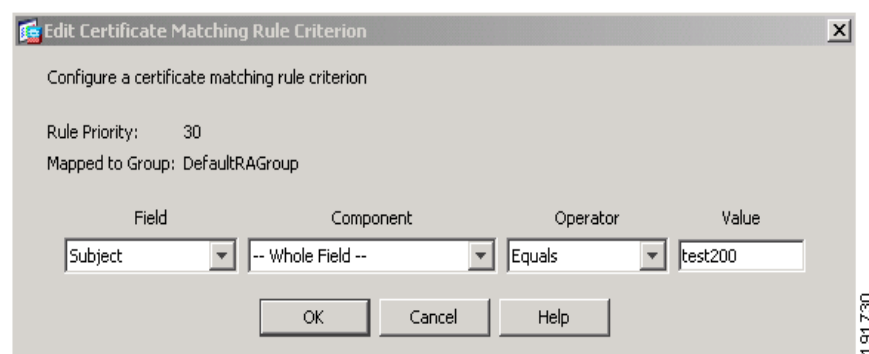
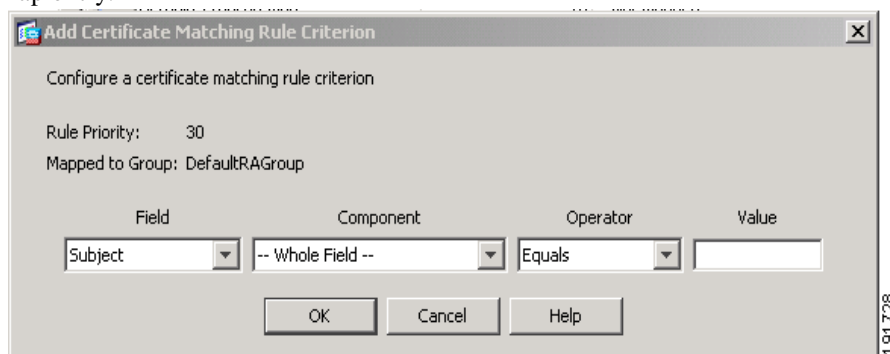
## Add/Edit Certificate Matching Rule

Use the **Add/Edit Certificate Matching Rule** dialog box to assign the name of a list (map) to a connection profile.

### Fields

- **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.
- **Rule Priority**—Type a decimal to specify the sequence with which the security appliance evaluates the map when it receives a connection request. For the first rule defined, the default priority is 10. The security appliance 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 security appliance ignores the map entry.



### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

### Add/Edit Certificate Matching Rule Criterion

Use the **Add/Edit Certificate Matching Rule Criterion** dialog box to configure a certificate matching rule criterion for the selected group.

#### Fields

- **Rule Priority**—(Display only). Sequence with which the security appliance evaluates the map when it receives a connection request. The security appliance 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.
- **Component**—(Applies only if Subject of Issuer is selected.) Select the distinguished name component used in the rule:

| DN Field                             | Definition                                                                                                               |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Whole Field</b>                   | The entire DN.                                                                                                           |
| <b>Country (C)</b>                   | The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.                              |
| <b>Common Name (CN)</b>              | The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy. |
| <b>DN Qualifier (DNQ)</b>            | A specific DN attribute.                                                                                                 |
| <b>E-mail Address (EA)</b>           | The e-mail address of the person, system or entity that owns the certificate.                                            |
| <b>Generational Qualifier (GENQ)</b> | A generational qualifier such as Jr., Sr., or III.                                                                       |
| <b>Given Name (GN)</b>               | The first name of the certificate owner.                                                                                 |
| <b>Initials (I)</b>                  | The first letters of each part of the certificate owner's name.                                                          |
| <b>Locality (L)</b>                  | The city or town where the organization is located.                                                                      |
| <b>Name (N)</b>                      | The name of the certificate owner.                                                                                       |
| <b>Organization (O)</b>              | The name of the company, institution, agency, association, or other entity.                                              |
| <b>Organizational Unit (OU)</b>      | The subgroup within the organization.                                                                                    |
| <b>Serial Number (SER)</b>           | The serial number of the certificate.                                                                                    |

| DN Field                    | Definition                                                                                                    |
|-----------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Surname (SN)</b>         | The family name or last name of the certificate owner.                                                        |
| <b>State/Province (S/P)</b> | The state or province where the organization is located.                                                      |
| <b>Title (T)</b>            | The title of the certificate owner, such as Dr.                                                               |
| <b>User ID (UID)</b>        | 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.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configure Site-to-Site Tunnel Groups

The Tunnel Groups window shows the attributes of the currently configured Site-to-Site tunnel groups, lets you select the delimiter to use when parsing tunnel group names, and lets you add, modify, or delete tunnel groups.

#### Fields

- **Add**—Opens the Add IPSec Site-to-Site Tunnel Group dialog box.
- **Edit**—Opens the Edit IPSec Site-to-Site Tunnel Group dialog box.
- **Delete**—Removes the selected tunnel group. There is no confirmation or undo.
- **Table of Tunnel Groups**—Lists the tunnel group name, CA Certificate, IPSec protocol status (enabled or disabled), and group policy applied for each configured tunnel group.
- **Group Delimiter**—Selects the delimiter character to use parsing tunnel group names from the usernames that are received when tunnels are being negotiated.

## Add/Edit Site-to-Site Connection

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, specify a connection name, select an interface, specify IKE peer and user authentication parameters, specify protected networks, and specify encryption algorithms.

### Fields

- Peer IP Address—Lets you specify an IP address and whether that address is static.
- Connection Name—Specifies the name assigned to this tunnel group. 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.
- IKE Authentication—Specifies the pre-shared key and ID certificate 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 identity certificate, if available, to use for authentication.
  - Manage—Opens the Manage CA Certificates window, 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.
- Protected Networks—Selects or specifies the local and remote network protected for this connection.
  - Local Network—Specifies the IP address of the local network.
  - ...—Opens the Browse Local Network dialog box, on which you can select a local network.
  - Remote Network—Specifies the IP address of the remote network.
  - ...—Opens the Browse Remote Network dialog box, on which you can select a remote network.
- Encryption Algorithm—Specifies the encryption algorithms to use in the IKE and IPSec proposals.
  - IKE Proposal—Specifies one or more encryption algorithms to use for the IKE proposal.
  - Manage—Opens the Configure IKE Proposals dialog box.
  - IPSec Proposal—Specifies one or more encryption algorithms to use for the IPSec proposal.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Adding or Editing a Site-to-Site Tunnel Group

The Add or Edit IPSec Site-to-Site Tunnel Group dialog box lets you specify attributes for the IPSec site-to-site connection that you are adding. In addition, you can select IKE peer and user authentication parameters, configure IKE keepalive monitoring, and select the default group policy.

### Fields

- **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 window, 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.
- **IKE Keepalive** —Enables and configures IKE keepalive monitoring. You can select only one of the following attributes.
  - **Disable Keep Alive**—Enables or disables IKE keep alives.
  - **Monitor Keep Alive**—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 security appliance 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 security appliance never initiates keepalive monitoring.
- **Default Group Policy**—Select the group policy and client protocols that you want to use as the default 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. IPSec connections and user accounts refer to the group-policy information.
  - **Group Policy**—Lists the currently configured group policies. The default value is DfltGrpPolicy.
  - **Manage**—Opens the Configure Group Policies window, on which you can view the configured group policies and add, edit, or delete group policies from the list.
  - **IPSec Protocol**—Enables or disables the IPSec protocol for use by this group policy.

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Crypto Map Entry

In this window, specify crypto parameters for the Connection Profile.

### Fields

- **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), Group 5 (1536-bits), and Group 7 (ECC).
- **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.

## Crypto Map Entry for Static Peer Address

In this window, specify crypto parameters for the Connection Profile when the Peer IP Address is a static address.

### Fields

- **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), Group 5 (1536-bits), and Group 7 (ECC).
- **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 select 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), Group 5 (1536-bits), and Group 7 (ECC).

## Managing CA Certificates

Clicking Manage under IKE Peer Authentication opens the Manage CA Certificates window. Use this window to view, add, edit, and delete entries on the list of CA certificates available for IKE peer authentication.

The Manage CA Certificates window 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.

### Fields

- **Add or Edit**—Opens the Install Certificate window or the Edit Certificate window, which let you specify information about and install a certificate.

- **Show Details**—Displays detailed information about a certificate that you select in the table.
- **Delete**—Removes the selected certificate from the table. There is no confirmation or undo.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Install Certificate

Use this window 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 on this window.**
- **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 window.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configure Options for CA Certificate

Use this window to specify details about retrieving CA Certificates for this IPSec remote access connection. The tabs on this window are: Revocation Check, CRL Retrieval Policy, CRL Retrieval Method, OCSP Rules, and Advanced.

### Revocation Check Tab

Use this tab to specify information about CA Certificate revocation checking.

**Fields**

- The radio buttons specify whether to check certificates for revocation. The values of these buttons are as follows:
  - Do not check certificates for revocation
  - 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.

## Add/Edit Remote Access Connections > Advanced > General

Use this window 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.

**Fields**

- 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@it.cisco.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 security appliance 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@it.cisco.com#VPNGroup`. If you choose this option, you must use either the # or ! character for the group delimiter because the security appliance cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

A Kerberos realm is a special case. The convention in naming a Kerberos realm is to capitalize the DNS domain name associated with the hosts in the Kerberos realm. For example, if users are in the `it.cisco.com` domain, you might call your Kerberos realm `IT.CISCO.COM`.

- 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 security appliance 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.
  - Override account-disabled indication from AAA server—Overrides an account-disabled indication from a AAA server.

**Note**

Allowing override account-disabled is a potential security risk.

- Enable notification upon password expiration to allow user to change password—Checking this check box makes the following two parameters available. You can select 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 select this option, you must also specify the number of days.

In either case, and, if the password expires without being changed, the security appliance 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 security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

This feature requires the use of MS-CHAPv2.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Client Addressing

To specify the client IP address assignment policy and assign address pools to all IPsec and SSL VPN connections, choose **Config > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing**. The **Add IPsec Remote Access Connection** or **Add SSL VPN Access Connection** opens. Use this window to add address pools and assign them to interfaces, and view, edit, or delete them. The table at the bottom of the window lists the configured interface-specific address pools.

To understand the fields in this window or its descendent windows, see the sections that follow this one. You can view or change the configuration of address pools and their assignment to interfaces, as follows:

- To view or change the configuration of address pools, click **Add** or **Edit** in the **Add IPsec Remote Access Connection** or **Add SSL VPN Access Connection** window. The **Assign Address Pools to Interface** window opens. This window lets you assign IP address pools to the interfaces configured on the security appliance. Click **Select**. The **Select Address Pools** window opens. Use this window to view the configuration of address pools. You can change their address pool configuration as follows:

- To add an address pool to the security appliance, choose **Add**. The Add IP Pool dialog box opens.
- To change the configuration of an address pool on the security appliance, choose **Edit**. The Edit IP Pool dialog box opens if the addresses in the pool are not in use.



**Note** 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 security appliance, select the entry in the table and click **Delete**.



**Note** 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** in the Add IPsec Remote Access Connection or Add SSL VPN Access Connection window. The Assign Address Pools to Interface window opens. Select the interface to be assigned an address pool. Click **Select** next to the Address Pools field. The Select Address Pools window 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 in the Add IPsec Remote Access Connection or Add SSL VPN Access Connection window and click Edit. The Assign Address Pools to Interface window 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 window 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 from the Add IPsec Remote Access Connection or Add SSL VPN Access Connection window, choose the entry and click **Delete**.

The Add IPsec Remote Access Connection and Add SSL VPN Access Connection windows and their descendent windows are identical. Use the following sections to understand or assign values to the fields in these windows:

- [Add IPsec Remote Access Connection and Add SSL VPN Access Connection](#)
- [Assign Address Pools to Interface](#)
- [Select Address Pools](#)
- [Add or Edit IP Pool](#)
- [Add or Edit IP Pool](#)

## Add IPsec Remote Access Connection and Add SSL VPN Access Connection

To access the Add IPsec Remote Access Connection and Add SSL VPN Access Connection windows, choose Config > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing.

### Fields

Use the following descriptions to assign values to the fields in this window:

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

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Assign Address Pools to Interface

Use the Assign Address Pools to Interface window to select an interface and assign one or more address pools to that interface. To access this window, choose **Config > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit**.

### Fields

Use the following descriptions to assign values to the fields in this window:

- **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, on which you can select 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Select Address Pools

The Select Address Pools window 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. To access this window, choose Config > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select.

### Fields

Use the following descriptions to assign values to the fields in this window:

- Add—Opens the Add IP Pool window, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool window, 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add or Edit IP Pool

The Add or Edit IP Pool window lets you specify or modify a range of IP addresses for client address assignment. To access this window, choose Config > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select > Add or Edit.

### Fields

Use the following descriptions to assign values to the fields in this window:

- 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.

### Modes

The following table shows the modes in which this feature is available:



| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > General Tab > Authentication

This dialog box is available for IPsec on Remote Access and Site-to-Site tunnel groups. The settings on this dialog box apply to the tunnel group globally across the security appliance. 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 select None. Selecting something other than None or Local makes available the Use LOCAL if Server Group Fails check box. To set the authentication server group per interface, click Advanced.
- **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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit SSL VPN Connection > General > Authorization

The settings on this dialog box apply to the connection (tunnel group) globally across the security appliance. This dialog box lets you configure the following attributes:

- **Authorization Server Group**—Lists the available authorization server groups, including the LOCAL group. You can also select None (the default). Selecting something other than None makes available the check box for Users must exist in authorization database to connect.
- **Users must exist in the authorization database to connect**—Tells the security appliance to allow only users in the authorization database to connect. By default this feature is disabled. You must have a configured authorization server to use this feature.
- **Interface-Specific Authorization Server Groups**—(Optional) Lets you configure authorization server groups on a per-interface basis. Interface-specific authorization server groups take precedence over the global server group. If you do not explicitly configure interface-specific authorization, authorization takes place only at the group level.
  - **Interface**—Select the interface on which to perform authorization. The standard interfaces are outside (the default), inside, and DMZ. If you have configured other interfaces, they also appear in the list.

- **Server Group**—Select an available, previously configured authorization server group or group of servers, including the LOCAL group. You can associate a server group with more than one interface.
- **Add**—Click Add to add the interface/server group setting to the table and remove the interface from the available list.
- **Remove**—Click Remove to remove the interface/server group from the table and restore the interface to the available list.
- **Authorization Settings**—Lets you set values for usernames that the security appliance 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**—Allows the use of the entire Distinguished Name (DN) as the username.
  - **Specify individual DN fields as the username**—Enables the use of individual DN fields as the username.
  - **Primary DN Field**—Lists all of the DN field identifiers for your selection.

| <b>DN Field</b>               | <b>Definition</b>                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Country (C)                   | Two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.                              |
| Common Name (CN)              | Name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy. |
| DN Qualifier (DNQ)            | Specific DN attribute.                                                                                               |
| E-mail Address (EA)           | E-mail address of the person, system or entity that owns the certificate.                                            |
| Generational Qualifier (GENQ) | Generational qualifier such as Jr., Sr., or III.                                                                     |
| Given Name (GN)               | First name of the certificate owner.                                                                                 |
| Initials (I)                  | First letters of each part of the certificate owner's name.                                                          |
| Locality (L)                  | City or town where the organization is located.                                                                      |
| Name (N)                      | Name of the certificate owner.                                                                                       |
| Organization (O)              | Name of the company, institution, agency, association, or other entity.                                              |
| Organizational Unit (OU)      | Subgroup within the organization.                                                                                    |
| Serial Number (SER)           | Serial number of the certificate.                                                                                    |
| Surname (SN)                  | Family name or last name of the certificate owner.                                                                   |
| State/Province (S/P)          | State or province where the organization is located.                                                                 |
| Title (T)                     | Title of the certificate owner, such as Dr.                                                                          |
| User ID (UID)                 | Identification number of the certificate owner.                                                                      |
| User Principal Name (UPN)     | Used with Smart Card certificate authentication.                                                                     |

- **Secondary DN Field**—Lists all of the DN field identifiers (see the foregoing table) for your selection and adds the option None for no selection.

## Add/Edit SSL VPN Connections > Advanced > Accounting

The settings on this dialog box apply to the connection (tunnel group) globally across the security appliance. This dialog box lets you configure the following attribute:

- **Accounting Server Group**—Lists the available accounting server groups. You can also select None (the default). LOCAL is not an option.
- **Manage**—Opens the Configure AAA Server Groups dialog box.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > General > Client Address Assignment

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment. The Add or Edit Tunnel Group window > General > Client Address Assignment dialog box, lets you configure the following Client Address Assignment attributes:

- **DHCP Servers**—Specifies a DHCP server to use. You can add up to 10 servers, one at a time.
  - **IP Address**—Specifies the IP address of a DHCP server.
  - **Add**—Adds the specified DHCP server to the list for client address assignment.
  - **Delete**—Deletes the specified DHCP server from the list for client address assignment. There is no confirmation or undo.
- **Address Pools**—Lets you specify up to 6 address pools, using the following parameters:
  - **Available Pools**—Lists the available, configured address pools you can choose.
  - **Add**—Adds the selected address pool to the list for client address assignment.
  - **Remove**—Moves the selected address pool from the Assigned Pools list to the Available Pools list.
  - **Assigned Pools**—Lists the address pools selected for address assignment.



**Note** To configure interface-specific address pools, click Advanced.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > General > Advanced

The Add or Edit Tunnel Group window, General, Advanced dialog box, lets you configure the following interface-specific attributes:

- Interface-Specific Authentication Server Groups—Lets you configure an interface and server group for authentication.
  - Interface—Lists available interfaces for selection.
  - Server Group—Lists authentication server groups available for this interface.
  - Use LOCAL if server group fails—Enables or disables fallback to the LOCAL database if the server group fails.
  - Add—Adds the association between the selected available interface and the authentication server group to the assigned list.
  - Remove—Moves the selected interface and authentication server group association from the assigned list to the available list.
  - Interface/Server Group/Use Fallback—Show the selections you have added to the assigned list.
- Interface-Specific Client IP Address Pools—Lets you specify an interface and Client IP address pool. You can have up to 6 pools.
  - Interface—Lists the available interfaces to add.
  - Address Pool—Lists address pools available to associate with this interface.
  - Add—Adds the association between the selected available interface and the client IP address pool to the assigned list.
  - Remove—Moves the selected interface/address pool association from the assigned list to the available list.
  - Interface/Address Pool—Shows the selections you have added to the assigned list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > IPSec for Remote Access > IPSec

On the Add or Edit Tunnel Group window for IPSec for Remote Access, the IPSec dialog box lets you configure or edit IPSec-specific tunnel group parameters.

### Fields

- Pre-shared Key—Lets you specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
- Trustpoint Name—Selects a trustpoint name, if any trustpoints are configured. A trustpoint is a representation of a certificate authority. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

- **Authentication Mode**—Specifies the authentication mode: none, xauth, or hybrid.
  - none—Specifies no authentication mode.
  - xauth—Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.
  - hybrid—Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method—such as RADIUS, TACACS+ or SecurID—for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:
    1. The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
    2. An extended authentication (xauth) exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

**Note**

Before setting the authentication type to hybrid, you must configure the authentication server and create a pre-shared key.

- **IKE Peer ID Validation**—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.
- **Enable sending certificate chain**—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- **ISAKMP 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 security appliance 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 security appliance never initiates keepalive monitoring.
- **Interface-Specific Authentication Mode**—Specifies the authentication mode on a per-interface basis.
  - **Interface**—Lets you select the interface name. 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 select the authentication mode, none, xauth, or hybrid, as above.
  - **Interface/Authentication Mode table**—Shows the interface names and their associated authentication modes that are selected.
  - **Add**—Adds an interface/authentication mode pair selection to the Interface/Authentication Modes table.
  - **Remove**—Removes an interface/authentication mode pair selection from the Interface/Authentication Modes table.

- **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 window) 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.
  - **Image URL**—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For Windows-based VPN clients, the URL must be of the form `http://` or `https://`. For ASA 5505 in client mode or VPN 3002 hardware clients, the URL must be of the form `tftp://`.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group for Site-to-Site VPN

The Add or Edit Tunnel Group dialog box lets you configure or edit tunnel group parameters for this Site-to-Site connection profile.

### Fields

- **Certificate Settings**—Sets the following certificate chain and IKE peer validation attributes:
  - **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 IKE (ISAKMP) keepalive monitoring.
  - **Disable Keepalives**—Enables or disables IKE keep alives.
  - **Monitor Keepalives**—Enables or disables IKE keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - **Confidence Interval**—Specifies the IKE keepalive confidence interval. This is the number of seconds the security appliance 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 IKE keepalive retries. The default is 2 seconds.
  - **Head end will never initiate keepalive monitoring**—Specifies that the central-site security appliance never initiates keepalive monitoring.

- Default Group Policy—Specifies the following group-policy attributes:
  - Group Policy—Selects a group policy to use as the default group policy. The default value is DfltGrpPolicy.
  - Manage—Opens the Configure Group Policies dialog box.
  - IPSec Protocol—Enables or disables the use of the IPSec protocol for this connection profile.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > PPP

On the Add or Edit Tunnel Group window for a IPSec remote access tunnel group, the PPP dialog box lets you configure or edit the authentication protocols permitted of a PPP connection. This dialog box applies *only* to IPSec remote access tunnel groups.

#### Fields

- 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 MA-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.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > IPSec for LAN to LAN Access > General > Basic

On the Add or Edit Tunnel Group window for Site-to-Site Remote Access, the General, Basic dialog box you can specify a name for the tunnel group that you are adding (Add function only) and select the group policy.

On the Edit Tunnel Group window, the General dialog box displays the name and type of the tunnel group you are modifying.

**Fields**

- **Name**—Specifies the name assigned to this tunnel group. For the Edit function, this field is display-only.
- **Type**—(*Display-only*) Displays the type of tunnel group you are adding or editing. The contents of this field depend on your selection on the previous window.
- **Group Policy**—Lists the currently configured group policies. The default value is the default group policy, DfltGrpPolicy.
- **Strip the realm (administrative domain) from the username before passing it on to the AAA server**—Enables or disables stripping the realm 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@it.cisco.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 security appliance 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@it.cisco.com#VPNGroup`. If you choose this option, you must use either the # or ! character for the group delimiter because the security appliance cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

A Kerberos realm is a special case. The convention in naming a Kerberos realm is to capitalize the DNS domain name associated with the hosts in the Kerberos realm. For example, if users are in the `it.cisco.com` domain, you might call your Kerberos realm `IT.CISCO.COM`.

- **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 security appliance 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.
  - **Override account-disabled indication from AAA server**—Overrides an account-disabled indication from a AAA server.

**Note**

Allowing override account-disabled is a potential security risk.

- **Enable notification upon password expiration to allow user to change password**—Checking this check box makes the following two parameters available. If you do not also check the Enable notification prior to expiration check box, the user receives notification only after the password has expired.



- Enable notification prior to expiration—When you check this option, the security appliance notifies the remote user at login that the current password is about to expire or has expired, 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 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 security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this does not change the number of days before the password expires, but rather, it enables the notification. If you check this check box, you must also specify the number of days.

- Notify...days prior to expiration—Specifies the number of days before the current password expires to notify the user of the pending expiration. The range is 1 through 180 days.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > IPSec for LAN to LAN Access > IPSec

The Add or Edit Tunnel Group window for IPSec for Site-to-Site access, IPSec dialog box, lets you configure or edit IPSec Site-to-Site-specific tunnel group parameters.

### Fields

- Name—Specifies the name assigned to this tunnel group. For the Edit function, this field is display-only.
- Type—(*Display-only*) Displays the type of tunnel group you are adding or editing. The contents of this field depend on your selection on the previous window.
- Pre-shared Key—Lets you specify the value of the pre-shared key for the tunnel group. The maximum length of the pre-shared key is 128 characters.
- Trustpoint Name—Selects a trustpoint name, if any trustpoints are configured. A trustpoint is a representation of a certificate authority. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.
- Authentication Mode—Specifies the authentication mode: none, xauth, or hybrid.
  - none—Specifies no authentication mode.
  - xauth—Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.
  - hybrid—Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method—such as RADIUS, TACACS+ or SecurID—for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:
    1. The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.

2. An extended authentication (xauth) exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

**Note**

Before setting the authentication type to hybrid, you must configure the authentication server and create a pre-shared key.

- IKE Peer ID Validation—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.
- Enable sending certificate chain—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- ISAKMP 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 security appliance 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 security appliance never initiates keepalive monitoring.
- Interface-Specific Authentication Mode—Specifies the authentication mode on a per-interface basis.
  - Interface—Lets you select the interface name. 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 select the authentication mode, none, xauth, or hybrid, as above.
  - Interface/Authentication Mode table—Shows the interface names and their associated authentication modes that are selected.
  - Add—Adds an interface/authentication mode pair selection to the Interface/Authentication Modes table.
  - Remove—Removes an interface/authentication mode pair selection from the Interface/Authentication Modes table.
- 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 window) 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.

- Image URL—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For Windows-based VPN clients, the URL must be of the form `http://` or `https://`. For ASA 5505 in client mode or VPN 3002 hardware clients, the URL must be of the form `tftp://`.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > Clientless SSL VPN Access > General > Basic

The Add or Edit pane, General, Basic dialog box lets you specify a name for the tunnel group that you are adding, lets you select the group policy, and lets you configure password management.

On the Edit Tunnel Group window, the General dialog box displays the name and type of the selected tunnel group. All other functions are the same as for the Add Tunnel Group window.

### Fields

- Name—Specifies the name assigned to this tunnel group. For the Edit function, this field is display-only.
- Type—Displays the type of tunnel group you are adding or editing. For Edit, this is a display-only field whose contents depend on your selection in the Add window.
- Group Policy—Lists the currently configured group policies. The default value is the default group policy, `DfltGrpPolicy`.
- Strip the realm —Not available for Clientless SSL VPN.
- Strip the group —Not available for Clientless SSL VPN.
- Password Management—Lets you configure parameters relevant to overriding an account-disabled indication from a AAA server and to notifying users about password expiration.
  - Override account-disabled indication from AAA server—Overrides an account-disabled indication from a AAA server.



### Note

Allowing override account-disabled is a potential security risk.

- Enable notification upon password expiration to allow user to change password—Checking this check box makes the following two parameters available. If you do not also check the Enable notification prior to expiration check box, the user receives notification only after the password has expired.
- Enable notification prior to expiration—When you check this option, the security appliance notifies the remote user at login that the current password is about to expire or has expired, 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 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 security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this does not change the number of days before the password expires, but rather, it enables the notification. If you check this check box, you must also specify the number of days.

- Notify...days prior to expiration—Specifies the number of days before the current password expires to notify the user of the pending expiration. The range is 1 through 180 days.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add/Edit Tunnel Group > Clientless SSL VPN > Basic

The attributes on the Add/Edit Tunnel Group General Tab dialog boxes for Clientless SSL VPN are the same as those for Add/Edit Tunnel Group General dialog boxes for IPsec Remote Access. The following description applies to the fields appearing on the Clientless SSL VPN dialog boxes.

### Fields

The Basic dialog box lets you configure the following attributes for Clientless SSL VPN:

- Authentication—Specifies the type of authentication to perform: AAA, Certificate, or Both. The default value is AAA.
- DNS Group—Specifies the DNS server to use for a connection profile. The default value is DefaultDNS.
- CSD Failure group policy—This attribute is valid only for security appliances with Cisco Secure Desktop installed. The security appliance uses this attribute to limit access rights to remote CSD clients if you use Cisco Secure Desktop Manager to set the VPN feature policy to one of the following options:
  - “Use Failure Group-Policy.”
  - “Use Success Group-Policy, if criteria match,” and the criteria fail to match.

This attribute specifies the name of the failure group policy to be applied. Choose a group policy to differentiate access rights from those associated with the default group policy. The default value is DfltGrpPolicy.



**Note** The security appliance does not use this attribute if you set the VPN feature policy to “Always use Success Group-Policy.”

For more information, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administration Guide*.

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Internal Group Policy IPSec Client Attributes

Use this window to specify whether to strip the realm and group from the username before passing them to the AAA server, and to specify password management options.

### Fields

- 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@it.cisco.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 security appliance 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@it.cisco.com#VPNGroup`. If you choose this option, you must use either the # or ! character for the group delimiter because the security appliance cannot interpret the @ as a group delimiter if it is also present as the realm delimiter.

A Kerberos realm is a special case. The convention in naming a Kerberos realm is to capitalize the DNS domain name associated with the hosts in the Kerberos realm. For example, if users are in the `it.cisco.com` domain, you might call your Kerberos realm `IT.CISCO.COM`.

- 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 security appliance 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.
  - Override account-disabled indication from AAA server—Overrides an account-disabled indication from a AAA server.

**Note**

Allowing override account-disabled is a potential security risk.

- Enable notification upon password expiration to allow user to change password—Checking this check box makes the following two parameters available. You can select 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 select this option, you must also specify the number of days.

In either case, and, if the password expires without being changed, the security appliance 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 security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring Client Addressing for SSL VPN Connections

Use this window 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 window. The table at the bottom of the window lists the configured interface-specific address pools.

**Fields**

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

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

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Assign Address Pools to Interface

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

#### Fields

- **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, on which you can select 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 window 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.

#### Fields

- **Add**—Opens the Add IP Pool window, on which you can configure a new IP address pool.
- **Edit**—Opens the Edit IP Pool window, 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.

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Add or Edit an IP Address Pool

Configures or modifies an IP address pool.

### Fields

- 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Authenticating SSL VPN Connections

The SSL VPN Connections > Advanced > Authentication window lets you configure authentication attributes for SSL VPN connections.

## System Options

The System Options pane lets you configure features specific to VPN sessions on the security appliance.

### Fields

- Enable inbound IPSec sessions to bypass interface access-lists. Group policy and per-user authorization access lists still apply to the traffic—By default, the security appliance allows VPN traffic to terminate on a security appliance 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 security appliance performance without any security risks. (Group policy and per-user authorization access lists 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.

- 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 Active IPsec VPN Sessions—Specifies the maximum number of active IPsec VPN sessions allowed. This field is active only when you select 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.
- Preserve stateful VPN flows when tunnel drops for Network-Extension Mode (NEM)—Enables or disables preserving IPsec tunneled flows in Network-Extension Mode. With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout window, 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).

#### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

## Configuring SSL VPN Connections, Advanced

The advanced options include configuring split tunneling, IE browser proxy, and group-policy related attributes for SSL VPN/AnyConnect clients and IPsec clients.

## Configuring Split Tunneling

Split tunneling lets you specify that certain data traffic is encrypted (“goes through the tunnel”), while the remainder is sent in the clear (unencrypted). Split-tunneling network lists distinguish networks that require traffic to go through the tunnel from those that do not require tunneling. the security appliance makes split-tunneling decisions based on a network list, which is an ACL consisting of a list of addresses on the private network.

Fields

- DNS Names—Specify one or more DNS names to which this policy applies.

- **Policy**—Selects the split-tunneling policy, specifying whether to include or exclude from the tunnel the indicated network lists. If you do not select Inherit, the default is Exclude Network List Below.
- **Network List**—Selects the networks to which to apply the split-tunneling policy. If you do not select Inherit, the default is --None--.
- **Manage**—Opens the ACL Manager dialog box, on which you can configure access control lists to use as network lists.
- **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 security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.
  - **Intercept**—Specifies whether to allow the DHCP Intercept to occur. If you do not select, Inherit, the default setting is No.
  - **Subnet Mask**—Selects the subnet mask to use.

## Zone Labs Integrity Server

The Zone Labs Integrity Server panel lets you configure the security appliance 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 security appliance 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.

The screenshot shows the 'Zone Labs Integrity Server' configuration window in Cisco ASDM. The breadcrumb trail at the top is 'Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Zone Labs Integrity Server'. The window title is 'Zone Labs Integrity Server'. Inside, the text 'Configure the Zone Labs Integrity Server parameters.' is displayed. The 'Server Parameters' section contains a 'Server IP address' field with an 'Add >>' button and a 'Delete' button. To the right of the IP address field is a large empty box and two buttons: 'Move Up' and 'Move Down'. Below this, the 'Server Port' is set to '5054' and the 'Interface' is set to '--None--'. Further down, the 'Fail Timeout' is set to '10' seconds and the 'SSL Certificate Port' is set to '80'. At the bottom of the configuration area are two checkboxes: 'Enable SSL Authentication' and 'Close connection on timeout', both of which are unchecked. At the very bottom of the window are 'Apply' and 'Reset' buttons. A vertical text '191722' is visible on the right edge of the window.

**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 security appliance and then reestablish the client VPN session.

**Fields**

- **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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 security appliance. By default, client SSL authentication is disabled.
- **Close connection on timeout**—Check to close the connection between the security appliance and the Integrity Server on a timeout. By default, the connection remains open.
- **Apply**—Click to apply the Integrity Server setting to the security appliance running configuration.
- **Reset**—Click to remove Integrity Server configuration changes that have not yet been applied.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

# Easy VPN Remote

Easy VPN Remote lets the ASA 5505 act as an Easy VPN client device. The ASA 5505 can then initiate a VPN tunnel to an Easy VPN server, which can be a security appliance, a Cisco VPN 3000 Concentrator, an IOS-based router, or a firewall acting as an Easy VPN server.

The Easy VPN client supports one of two modes of operation: Client Mode or Network Extension Mode (NEM). The mode of operation determines whether the Easy VPN Client inside hosts are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because Easy VPN Client does not have a default mode.

Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the Easy VPN Client private network from those on the enterprise network. The Easy VPN Client performs Port Address Translation (PAT) for all VPN traffic for its inside hosts. IP address management is neither required for the Easy VPN Client inside interface or the inside hosts.

NEM makes the inside interface and all inside hosts routable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or via DHCP) pre-configured with static IP addresses. PAT does not apply to VPN traffic in NEM. This mode does not require a VPN configuration for each client. The Cisco ASA 5505 configured for NEM mode supports automatic tunnel initiation. The configuration must store the group name, user name, and password. Automatic tunnel initiation is disabled if secure unit authentication is enabled.

The network and addresses on the private side of the Easy VPN Client are hidden, and cannot be accessed directly.

## Fields

- Enable Easy VPN Remote—Enables the Easy VPN Remote feature and makes available the rest of the fields on this window for configuration.
- Mode—Selects either Client mode or Network extension mode.
  - Client mode—Uses Port Address Translation (PAT) mode to isolate the addresses of the inside hosts, relative to the client, from the enterprise network.
  - Network extension mode—Makes those addresses accessible from the enterprise network.



### Note

If the Easy VPN Remote is using NEM and has connections to secondary servers, establish an ASDM connection to each headend and check Enable Reverse Route Injection on the Configuration > VPN > IPSec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced dialog box to configure dynamic announcements of the remote network using RRI.

- Auto connect—The Easy VPN Remote establishes automatic IPSec data tunnels unless both of the following are true: Network extension mode is configured locally, and split-tunneling is configured on the group policy pushed to the Easy VPN Remote. If both are true, checking this attribute automates the establishment of IPSec data tunnels. Otherwise, this attribute has no effect.
- Group Settings—Specifies whether to use a pre-shared key or an X.509 certificate for user authentication.
  - Pre-shared key—Enables the use of a pre-shared key for authentication and makes available the subsequent Group Name, Group Password, and Confirm Password fields for specifying the group policy name and password containing that key.
  - Group Name—Specifies the name of the group policy to use for authentication.

- Group Password—Specifies the password to use with the specified group policy.
- Confirm Password—Requires you to confirm the group password just entered.
- X.509 Certificate—Specifies the use of an X.509 digital certificate, supplied by a Certificate Authority, for authentication.
- Select Trustpoint—Lets you select a trustpoint, which can be an IP address or a hostname, from the drop-down list. To define a trustpoint, click the link to Trustpoint(s) configuration at the bottom of this area.
- Send certificate chain—Enables sending a certificate chain, not just the certificate itself. This action includes the root certificate and any subordinate CA certificates in the transmission.
- User Settings—Configures user login information.
  - User Name—Configures the VPN username for the Easy VPN Remote connection. Xauth provides the capability of authenticating a user within IKE using TACACS+ or RADIUS. Xauth authenticates a user (in this case, the Easy VPN hardware client) using RADIUS or any of the other supported user authentication protocols. The Xauth username and password parameters are used when secure unit authentication is disabled and the server requests Xauth credentials. If secure unit authentication is enabled, these parameters are ignored, and the security appliance prompts the user for a username and password.
  - User Password—Configures the VPN user password for the Easy VPN Remote connection.
  - Confirm Password—Requires you to confirm the user password just entered.
- Easy VPN Server To Be Added—Adds or removes an Easy VPN server. Any ASA or VPN 3000 Concentrator Series can act as a Easy VPN server. A server must be configured before a connection can be established. The security appliance supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order. The first server in the Easy VPN Server(s) list is the primary server. You can specify a maximum of ten backup servers in addition to the primary server.
  - Name or IP Address—The name or IP address of an Easy VPN server to add to the list.
  - Add—Moves the specified server to the Easy VPN Server(s) list.
  - Remove—Moves the selected server from the Easy VPN Server(s) list to the Name or IP Address file. Once you do this, however, you cannot re-add the same address unless you re-enter the address in the Name or IP Address field.
  - Easy VPN Server(s)—Lists the configured Easy VPN servers in priority order.
  - Move Up/Move Down—Changes the position of a server in the Easy VPN Server(s) list. These buttons are available only when there is more than one server in the list.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |

# Advanced Easy VPN Properties

## Device Pass-Through

Certain devices like Cisco IP phones, printers, and the like are incapable of performing authentication, and therefore of participating in individual unit authentication. To accommodate these devices, the device pass-through feature, enabled by the MAC Exemption attributes, exempts devices with the specified MAC addresses from authentication when Individual User Authentication is enabled.

The first 24 bits of the MAC address indicate the manufacturer of the piece of equipment. The last 24 bits are the unit's serial number in hexadecimal format.

## Tunneled Management

When operating an ASA model 5505 device behind a NAT device, use the Tunneled Management attributes to specify how to configure device management— in the clear or through the tunnel—and specify the network or networks allowed to manage the Easy VPN Remote connection through the tunnel. The public address of the ASA 5505 is not accessible when behind the NAT device unless you add static NAT mappings on the NAT device.

When operating a Cisco ASA 5505 behind a NAT device, use the **vpnclient management** command to specify how to configure device management— with additional encryption or without it—and specify the hosts or networks to be granted administrative access. The public address of the ASA 5505 is not accessible when behind the NAT device unless you add static NAT mappings on the NAT device.

## Fields

- **MAC Exemption**—Configures a set of MAC addresses and masks used for device pass-through for the Easy VPN Remote connection
  - **MAC Address**—Exempts the device with the specified MAC address from authentication. The format for specifying the MAC address this field uses three hex digits, separated by periods; for example, 45ab.ff36.9999.
  - **MAC Mask**—The format for specifying the MAC mask in this field uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.
  - **Add**—Adds the specified MAC address and mask pair to the MAC Address/Mask list.
  - **Remove**—Moves the selected MAC address and mask pair from the MAC Address/MAC list to the individual MAC Address and MAC Mask fields.
- **Tunneled Management**—Configures IPSec encryption for device management and specifies the network or networks allowed to manage the Easy VPN hardware client connection through the tunnel. Selecting Clear Tunneled Management merely removes that IPSec encryption level and does not affect any other encryption, such as SSH or https, that exists on the connection.
  - **Enable Tunneled Management**—Adds a layer of IPSec encryption to the SSH or HTTPS encryption already present in the management tunnel.
  - **Clear Tunneled Management**—Uses the encryption already present in the management tunnel, without additional encryption.
  - **IP Address**— Specifies the IP address of the host or network to which you want to grant administrative access to the Easy VPN hardware client through the VPN tunnel. You can individually add one or more IP addresses and their respective network masks.
  - **Mask**—Specifies the network mask for the corresponding IP address.

- Add—Moves the specified IP address and mask to the IP Address/Mask list.
- Remove—Moves the selected IP address and mask pair from the IP Address/Mask list to the individual IP Address and Mask fields in this area.
- IP Address/Mask—Lists the configured IP address and mask pairs to be operated on by the Enable or Clear functions in this area.
- IPSec Over TCP—Configure the Easy VPN Remote connection to use TCP-encapsulated IPSec.
  - Enable—Enables IPSec over TCP.



**Note** Choose Configuration > VPN > IPSec > Pre-Fragmentation, double-click the outside interface, and set the DF Bit Setting Policy to Clear if you configure the Easy VPN Remote connection to use TCP-encapsulated IPSec. The Clear setting lets the security appliance send large packets.

- Enter Port Number—Specifies the port number to use for the IPSec over TCP connection.
- Server Certificate—Configures the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map. Use this parameter to enable Easy VPN server certificate filtering. To define a certificate map, go to Configuration > VPN > IKE > Certificate Group Matching > Rules.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | —           | •                | —        | —      |



# CHAPTER 36

## Configuring Dynamic Access Policies

---

This chapter describes how to configure dynamic access policies. It includes the following sections.

- [Understanding VPN Access Policies](#)
- [Add/Edit Dynamic Access Policies](#)
- [Add/Edit AAA Attributes](#)
- [Retrieve AD Groups from selected AD Server Group](#)
- [Add/Edit Endpoint Attributes](#)
- [Operator for Endpoint Category](#)
- [DAP Examples](#)

## Understanding VPN 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 security appliance 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 security appliance grants access to a particular user for a particular session based on the policies you define. It 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 security appliance uses for selecting and applying DAP records during session establishment. Stored on the security appliance. You can use ASDM to modify it and upload it to the security appliance 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.

For more information about Dynamic Access Policies, click the following links:

- [DAP Support for Remote Access Connection Types](#)
- [DAP and AAA](#)
- [DAP and Endpoint Security](#)
- [DAP Connection Sequence](#)
- [Test Dynamic Access Policies](#)
- [DAP Examples](#)

## Configuring Dynamic Access Policies

To configure dynamic access policies, in the Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies pane in ASDM, perform the following steps:

- 
- Step 1** To include certain antivirus, antispy, or personal firewall endpoint attributes, click the [CSD configuration](#) link near the top of the pane. Then enable Cisco Secure Desktop *and* Host Scan extensions. This link does not display if you have previously enabled both of these features.
- If you enable Cisco Secure Desktop, but do not enable Host Scan extensions, when you apply your changes ASDM includes a link to enable [Host Scan configuration](#).
- Step 2** To create a new dynamic access policy, click **Add**. To modify an existing policy, click **Edit**.
- Step 3** To test already configured policies, click **Test Dynamic Access Policies**.
- 

### Fields

- **Priority**—Displays the priority of the DAP record. The security appliance uses this value to logically sequence the access lists when aggregating the network and web-type ACLs from multiple DAP records. The security appliance 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 access list that applies to the session.
- **Web-Type ACL List**—Displays the name of the SSL VPN access list that applies to the session.
- **Description**—Describes the purpose of the DAP record.
- **Test Dynamic Access Policies button**—Click to test already configured DAP records.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## DAP Support for Remote Access Connection Types

The DAP system supports the following remote access methods:

- IPsec VPN
- Clientless (browser-based) SSLVPN
- Cisco AnyConnect SSL VPN
- PIX cut-through proxy (posture assessment not available)

## DAP and AAA

DAP complements AAA services. It provides a limited set of authorization attributes that can override those AAA provides. The security appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The security appliance can select multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the security appliance receives from a RADIUS or LDAP server. For more information about DAP and AAA, see the section, [Add/Edit AAA Attributes](#).

### AAA Attribute Definitions

[Table 36-1](#) 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.

**Table 36-1** AAA Selection Attributes for DAP Use

| Attribute Type | Attribute Name        | Source | Value  | Max String Length | Description                                                                                                    |
|----------------|-----------------------|--------|--------|-------------------|----------------------------------------------------------------------------------------------------------------|
| Cisco          | aaa.cisco.class       | AAA    | string | 64                | Group policy name on the security appliance 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)                        |
|                | 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)                           |

**Table 36-1 AAA Selection Attributes for DAP Use (continued)**

|        |                     |        |        |     |                             |
|--------|---------------------|--------|--------|-----|-----------------------------|
| LDAP   | aaa.ldap.<label>    | LDAP   | string | 128 | LDAP attribute value pair   |
| RADIUS | aaa.radius.<number> | RADIUS | string | 128 | Radius attribute value pair |

Refer to [Security Appliance Supported RADIUS Attributes and Values](#) for a table that lists RADIUS attributes that the security appliance supports.

## DAP and Endpoint Security

The security appliance obtains endpoint security attributes by using posture assessment methods that you configure. These include Cisco Secure Desktop and NAC. For details, see the Cisco Secure Desktop section of ASDM. [Table 36-2](#) identifies each of the remote access protocols DAP supports, the posture assessment tools available for that method, and the information that tool provides.

**Table 36-2 DAP Posture Assessment**

| Remote Access Protocol | Cisco Secure Desktop                                                                | Host Scan                                                                  | NAC                | Cisco NAC Appliance            |
|------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------|--------------------------------|
|                        | Returns files information, registry key values, running processes, operating system | Returns antivirus, antispyware, and personal firewall software information | Returns NAC status | Returns VLAN Type and VLAN IDs |
| IPsec VPN              | — <sup>1</sup>                                                                      | —                                                                          | X                  | X                              |
| Cisco AnyConnect VPN   | X                                                                                   | X                                                                          | X                  | X                              |
| Clientless VPN         | X                                                                                   | X                                                                          | —                  | —                              |
| PIX Cut-through Proxy  | —                                                                                   | —                                                                          | —                  | —                              |

1. — indicates no; X indicates yes

### Endpoint Attribute Definitions

[Table 36-3](#) defines the endpoint 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 area in the Add/Edit Dynamic Access Policy pane. The *label* variable identifies the application, filename, process, or registry entry.

**Table 36-3 Endpoint Attribute Definitions**

| Attribute Type                              | Attribute Name                         | Source    | Value   | Max String Length | Description                                     |
|---------------------------------------------|----------------------------------------|-----------|---------|-------------------|-------------------------------------------------|
| Antispyware (Requires Cisco Secure Desktop) | endpoint.as. <i>label</i> .exists      | Host Scan | true    | —                 | Antispyware program exists                      |
|                                             | endpoint.as. <i>label</i> .version     |           | string  | 32                | Version                                         |
|                                             | endpoint.as. <i>label</i> .description |           | string  | 128               | Antispyware description                         |
|                                             | endpoint.as. <i>label</i> .lastupdate  |           | integer | —                 | Seconds since update of antispyware definitions |

**Table 36-3** *Endpoint Attribute Definitions (continued)*

| Attribute Type                                 | Attribute Name                   | Source         | Value        | Max String Length | Description                                                                                |
|------------------------------------------------|----------------------------------|----------------|--------------|-------------------|--------------------------------------------------------------------------------------------|
| Antivirus<br>(Requires Cisco Secure Desktop)   | endpoint.av.label.exists         | Host Scan      | true         | —                 | Antivirus program exists                                                                   |
|                                                | endpoint.av.label.version        |                | string       | 32                | Version                                                                                    |
|                                                | endpoint.av.label.description    |                | string       | 128               | Antivirus description                                                                      |
|                                                | endpoint.av.label.lastupdate     |                | integer      | —                 | Seconds since update of antivirus definitions                                              |
| Application                                    | endpoint.application.clienttype  | Application    | string       | —                 | Client type:<br>CLIENTLESS<br>ANYCONNECT<br>IPSEC<br>L2TP                                  |
| File                                           | endpoint.file.label.exists       | Secure Desktop | true         | —                 | The files exists                                                                           |
|                                                | 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                                                                 |
| Operating System                               | endpoint.os.version              | Secure Desktop | string       | 32                | Operating system                                                                           |
|                                                | endpoint.os.servicepack          |                | integer      | —                 | Service pack for Windows                                                                   |
| Personal firewall<br>(Requires Secure Desktop) | endpoint.fw.label.exists         | Host Scan      | true         | —                 | The personal firewall exists                                                               |
|                                                | endpoint.fw.label.version        |                | string       | 32                | Version                                                                                    |
|                                                | endpoint.fw.label.description    |                | string       | 128               | Personal firewall description                                                              |
| Policy                                         | endpoint.policy.location         | Secure Desktop | string       | 64                | Location value from Cisco Secure Desktop                                                   |
| Process                                        | endpoint.process.label.exists    | Secure Desktop | true         | —                 | The process exists                                                                         |
|                                                | endpoint.process.label.path      |                | string       | 255               | Full path of the process                                                                   |
| Registry                                       | endpoint.registry.label.type     | Secure Desktop | dword string | —                 | dword                                                                                      |
|                                                | endpoint.registry.label.value    |                | string       | 255               | Value of the registry entry                                                                |
| VLAN                                           | endoint.vlan.type                | CNA            | string       | —                 | VLAN type:<br>ACCESS<br>AUTH<br>ERROR<br>GUEST<br>QUARANTINE<br>ERROR<br>STATIC<br>TIMEOUT |

## DAP and Anti-Virus, Anti-Spyware, 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 Host Scan modules of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes.

Most, but not all, anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan 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, Host Scan 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, Host Scan 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, Host Scan ignores the presence of the software. The security appliance does not select 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.

## DAP Connection Sequence

The following sequence outlines a typical remote access connection establishment.

1. A remote client attempts a VPN connection.
2. The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.
3. The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.
4. The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.
5. The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information.
6. The security appliance aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The security appliance applies the DAP policy to the session.

## 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. To specify these pairs, use the Add/Edit buttons associated with the AAA Attribute and Endpoint Attribute tables. 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.

When you enter attribute value pairs and 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” text area.

### Fields

- **Selection Criteria**—Determine the AAA and endpoint attributes to test for dynamic access policy retrieval.
- **AAA Attributes**
  - **AAA Attribute**—Identifies the AAA attribute.
  - **Operation Value**—Identifies the attribute as  $\neq$  to the given value.
  - **Add/Edit**—Click to add or edit a AAA attribute.
- **Endpoint Attributes**—Identifies the endpoint attribute.
  - **Endpoint ID**—Provides the endpoint attribute ID.
  - **Name/Operation/Value**—
  - **Add/Edit/Delete**—Click to add, edit or delete and endpoint attribute.
- **Test Result**—Displays the result of the test.
- **Test**—Click to test the retrieval of the policies you have set.
- **Close**—Click to close the pane.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Add/Edit Dynamic Access Policies

To add or edit a dynamic access policy, perform the following steps:

- Step 1** At the top of the **Add/Edit Dynamic Access Policy** pane, provide a name (required) and a description (optional) of this dynamic access policy.
- Step 2** In the **Priority** field, set a priority for the dynamic access policy. The security appliance applies access policies in the order you set here, highest number having the highest priority. In the case of DAP records with the same priority setting and conflicting ACL rules, the most restrictive rule applies.
- Step 3** In the **Add/Edit AAA Attributes** field, use the ANY/ALL/NONE drop-down box (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.
- Step 4** To Set AAA attributes, click **Add/Edit** in the AAA Attributes field.
- Step 5** Before you set endpoint attributes, configure CSD Host Scan.
- Step 6** To set endpoint security attributes, click **Add/Edit** in the Endpoint ID field.
- Step 7** You can create multiple instances of each type of endpoint attribute. For each of these types, you need to decide whether the DAP policy should require that the user have all instances of a type (Match all = AND) or only one of them (Match Any = OR). To set this value for each of the end point attributes, click the **Logical Op.** button.

- Step 8** In the **Advanced** field you can enter one or more logical expressions to set AAA or endpoint attributes other than what is possible in the AAA and Endpoint areas above.
- Step 9** To configure network and webtype ACLs, file browsing, file server entry, HTTP proxy, URL entry, port forwarding lists and URL lists, set values in the **Access Policy Attributes** fields.

### Fields

- Policy Name—A string of 4 through 32 characters, no spaces allowed.
- Description—(Optional) Describes the purpose of the DAP record. Maximum 80 characters.
- Priority—Sets the priority of the DAP. The security appliance applies access policies in the order you set here, highest number having the highest priority. Values of 0 to 2147483647 are valid. Default = 0.
- ANY/ALL/NONE drop-down box—Set to require that user authorization attributes match any, all, or none of the values in the AAA attributes you are configuring, 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 security appliance always selects it since all selection criteria are satisfied.
- AAA Attributes—Displays the configured AAA attributes.
  - Attribute—Displays the name of the AAA attribute.
  - Operation/Value—= !=
  - Add/Edit/Delete —Click to add, edit, or delete the highlighted AAA attribute.
- Endpoint Attributes—Displays the configured endpoint attributes
  - Endpoint ID—Identifies endpoint attributes.
  - Name/Operation/Value—Summarizes configured values for each endpoint attribute.
  - Add/Edit/Delete—Click to add, edit, or delete the highlighted endpoint attribute.



### Note

Cisco Secure Desktop provides the security appliance with all endpoint attributes except Application and NAC. To configure all other endpoint attributes, you must first enable Cisco Secure Desktop, and configure the relevant endpoint attributes there as well.

- Logical Op.—You can create multiple instances of each type of endpoint attribute. Click to configure whether the DAP policy should require that the user have all instances of a type (Match all = AND) or only one of them (Match Any = OR). Be aware that for some endpoint attributes, for example OS, it can never happen that a user would have more than one instance of the attribute.
- Advanced—Click to set additional attributes for the dynamic access policy. Be aware that this is an advanced feature that requires knowledge of Lua.
- 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 security appliance processes it, discarding any expressions it cannot parse.
- Guide—Click to display online help for creating these logical operations.

- Access Policy Attributes—These tabs let you set attributes for network and webtype ACL filters, file access, HTTP proxy, URL entry and lists, port forwarding, and clientless SSL VPN access methods. 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.
- Action Tab
  - Action—Specifies special processing to apply to a specific connection or session.
  - Continue—(Default) Click to apply access policy attributes to the session.
  - 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 128 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.

**Note**

You can include in such messages URLs or other embedded text, which require that you use the correct HTML tags.

For example: All contractors please read <a href='http://wwwin.abc.com/procedure.html'>Instructions</a> for the procedure to upgrade your antivirus software.

- Network ACL Filters Tab—Lets you select and 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 security appliance rejects it.
  - Network ACL drop-down box—Select already configured network ACLs to add to this DAP record. Only ACLs having all permit or all deny rules are eligible, and these are the only ACLs that display here.
  - 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 box 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 security appliance unless you first delete it from DAP records.
- Web-Type ACL Filters Tab—Lets you select and 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 security appliance rejects it.
  - Web-Type ACL drop-down box—Select already configured web-type ACLs to add to this DAP record. Only ACLs having all permit or all deny rules are eligible, and these are the only ACLs that display here.
  - 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 box 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 security appliance unless you first delete it from DAP records.
- Functions Tab—Lets you 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.



**Note** Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS.



**Note** 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, and use clientless SSL VPN to access those websites.

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's PC or workstation and the security appliance 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 security appliance to the destination web server is not secured.

In a clientless VPN connection, the security appliance 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 security appliance 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 security appliance 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, select 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.
- Port Forwarding Lists Tab—Lets you select and 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) 1.4+ 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 box—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 box 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 security appliance unless you first delete it from DAP records.
- URL Lists Tab—Lets you select and configure URL lists for user sessions.
  - Enable URL Lists—Click to enable. When this box is not selected, no URL lists display on the portal page for the connection.
  - URL List drop-down box—select already configured URL lists to add to the DAP record.
  - Manage...—Click to add, import, export, and delete URL lists.
  - URL Lists (unlabeled)—Displays the URL lists for the DAP record.
  - Add—Click to add the selected URL list from the drop-down box to the URL list box on the right.
  - Delete—Click to delete the selected URL list from the URL list box. You cannot delete a URL list from the security appliance unless you first delete it from DAP records.
- Access Method Tab—Lets you configure the type of remote access permitted.
  - Unchanged—Continue with the current remote access method.
  - AnyConnect Client—Connect using the Cisco AnyConnect VPN 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.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Add/Edit AAA Attributes

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](#).

### Fields

AAA Attributes Type—Use the drop down box to select 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 user on the security appliance or sent from a Radius/LDAP server as the IETF-Class (25) attribute. Maximum 64 characters.
  - IP Address—The assigned IP address for full tunnel VPN clients (IPsec, L2TP/IPsec, SSL VPN AnyConnect). Does not apply to Clientless SSL VPN, since there is no address assignment for clientless sessions.
  - 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 authentication/authorization.
  - =/!=—Equal to/Not equal to
- LDAP—The LDAP client 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.

LDAP attributes consist of an attribute name and attribute value pair in the DAP record.

- **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. Refer to [Security Appliance Supported RADIUS Attributes and Values](#) for a table that lists RADIUS attributes that the security appliance supports.



**Note** For RADIUS attributes, DAP defines the Attribute ID = 409 + 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).
  - `=/!=`—Equal to/Not equal to
- LDAP includes the Get AD Groups button. This button queries the LDAP server

The **show ad-groups** command applies only to Active Directory servers using LDAP. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

The default time that the security appliance 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.



**Note** If the Active Directory server has a large number of groups, the output of the **show ad-groups** command might be truncated based on limitations to the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

## Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Retrieve AD Groups from selected AD Server Group

You can query an Active Directory server for available AD groups in this window. This feature applies only to Active Directory servers using LDAP. Use the group information to specify dynamic access policy AAA selection criteria.

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 window. You can also change the time that the security appliance waits for a response from the server in the window. To configure these features, go to: 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 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.

**Fields**

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.

**Modes**

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

## Add/Edit Endpoint Attributes

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The security appliance dynamically generates a collection of endpoint attributes during session establishment, and stores these attributes in a database associated with the session. There is no limit for the number of endpoint attributes for each DAP record.

Each DAP record specifies the endpoint selection attributes that must be satisfied for the security appliance to select it. The security appliance selects only DAP records that satisfy every condition configured.

For detailed information about Endpoint attributes, click the following link:

- [Endpoint Attribute Definitions](#)

To configure endpoint attributes as selection criteria for DAP records, in the **Add/Edit Endpoint Attribute** dialog box, set components. These components change according to the attribute type you select.

### Fields

- **Endpoint Attribute Type**—Select from the drop-down list the endpoint attribute you want to set. Options include Antispyware, Antivirus, Application, File, NAC, Operating System, Personal Firewall, Process, Registry, VLAN, and Priority.

Endpoint attributes include these components, but not all attributes include all components. The following descriptions show (in parentheses) the attributes to which each component applies.

- **Exists/Does not exist buttons** (Antispyware, Antivirus, Application, File, NAC, Operating System, Personal Firewall, Process, Registry, VLAN, Priority)—Click the appropriate 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.
- **Vendor ID** (Antispyware, Antivirus, Personal Firewall)—Identify the application vendor.
- **Vendor Description** (Antispyware, Antivirus, Personal Firewall)—Provide text that describes the application vendor.
- **Version** (Antispyware, Antivirus, Personal Firewall)—Identify the version of the application, and specify whether you want the endpoint attribute to be equal to/not equal to that version.
- **Last Update** (Antispyware, Antivirus, File)—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.
- **Client Type** (Application)—Indicate the type of remote access connection, AnyConnect, Clientless, Cut-through Proxy, IPsec, or L2TP.
- **Checksum** (File)—Select the file and click the Compute Checksum button to arrive at this value.
- **Compute CRC32 Checksum** (File)—Use this calculator to determine the checksum value of a file.
- **Posture Status** (NAC)—Contains the posture token string received from ACS.
- **OS Version** (Operating System)—Windows (various), MAC, Linux, Pocket PC.
- **Service Pack** (Operating System)—Identify the service pack for the operating system.
- **Endpoint ID** (File, Process, Registry)—A string that identifies an endpoint for files, processes or registry entries. DAP uses this ID to match Cisco Secure Desktop host scan attributes for DAP selection. You must configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
- **Path** (Process, Policy)—Configure Host Scan before you configure this attribute. When you configure Host Scan, the configuration displays in this pane, so you can select it, reducing the possibility of errors in typing or syntax.
- **Value** (Registry)—dword or string
- **Caseless** (Registry)—Select to disregard case in registry entries.
- **VLAN ID** (VLAN)—A valid 802.1q number ranging from 1 to 4094
- **VLAN Type** (VLAN)—Possible values include the following:

|         |                                                 |
|---------|-------------------------------------------------|
| ACCESS  | Posture assessment passed                       |
| STATIC  | No posture assessment applied                   |
| TIMEOUT | Posture assessment failed due to no response    |
| AUTH    | Posture assessment still active                 |
| GUEST   | Posture assessment passed, switch to guest VLAN |

|            |                                                      |
|------------|------------------------------------------------------|
| QUARANTINE | Posture assessment failed, switch to quarantine VLAN |
| ERROR      | Posture assessment failed due to fatal error         |

- Policy (Location)—Enter the Cisco Secure Desktop Microsoft Windows location profile, case sensitive.

### Modes

The following table shows the modes in which this feature is available:

| Firewall Mode |             | Security Context |          |        |
|---------------|-------------|------------------|----------|--------|
| Routed        | Transparent | Single           | Multiple |        |
|               |             |                  | Context  | System |
| •             | •           | •                | —        | —      |

### Guide

This section provides information about constructing logical expressions for AAA or Endpoint attributes. Be aware that doing so requires sophisticated knowledge of Lua ([www.lua.org](http://www.lua.org)).

In the text box 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 security appliance 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 security appliance 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 j

appropriate logical expressions in Lua and enter them here.

- For a list of AAA Selection attributes, including proper name syntax for creating logical expressions, see [Table 36-1](#).
- For a list of endpoint selection attributes, including proper name syntax for creating logical expressions, see [Table 36-3](#).

### Syntax for Creating Lua EVAL Expressions

This section provides information about the syntax for creating Lua EVAL expressions.



#### Note

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 <a href="#">Table 36-1</a> and <a href="#">Table 36-3</a> 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                                               |
|         | "caseless"                                                                           | 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             |

**Example:**

```
EVAL(endpoint.os.version, "EQ", "Windows XP", "string")
```

**Constructing DAP Logical Expressions**

Study these examples for help in creating logical expressions in Lua.

- This AAA Lua expression tests for a match on usernames that begin with "b". It uses the string library and a regular expression:

```
(string.find(aaa.cisco.username, "^b") ~= nil)
```



**Note** The *string.find* expression does not work with multivalued attributes. See the [Group Membership Example](#) for an example that uses a multivalued attribute.

- This endpoint expression tests for a match on CLIENTLESS OR CVC client types:

```
(EVAL(endpoint.application.clienttype, "EQ", "CLIENTLESS") or
EVAL(endpoint.application.clienttype, "EQ", "CVC"))
```

- This endpoint expression tests for Norton Antivirus versions 10.x but excludes 10.5.x:

```
(EVAL(endpoint.av["NortonAV"].version, "GE", "10", "version") and
(EVAL(endpoint.av["NortonAV"].version, "LT", "10.5", "version") or
EVAL(endpoint.av["NortonAV"].version, "GE", "10.6", "version")))
```

**The DAP CheckAndMsg Function**

CheckAndMsg is a Lua function that you can configure DAP to call. It generates a user message based on a condition.



You use ASDM to configure CheckAndMsg through the Advanced field in DAP. The security appliance displays the message to the user only when the DAP record containing the LUA CheckAndMsg function is selected and results in a clientless SSL VPN or AnyConnect 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 appliances uses it to determine whether to select the DAP record. If the record is selected and results in termination, the security appliance displays the appropriate message.

### Checking for a Single Antivirus Program

This example checks if a single antivirus program, in this case McAfee, is installed on the user PC, and displays a message if it is not.

```
(CheckAndMsg(EVAL(endpoint.av.McAfeeAV.exists,"NE","true"),"McAfee AV was not found on your computer", nil))
```

### Checking for Antivirus Definitions Within the Last 10 Days

This example checks antivirus definitions within the last 10 days (864000 sec), in particular the last update of the McAfee AV dat file, and displays a message to a user lacking the appropriate update that they need an antivirus update:

```
((CheckAndMsg(EVAL(endpoint.av.McAfeeAV.lastupdate,"GT","864000","integer"),"AV Update needed! Please wait for the McAfee AV till it loads the latest dat file.",nil)))
```

### Checking for a Hotfix on the User PC

This example checks for a specific hotfix. If a user does not have the hotfix on their PC, a message that it is not installed displays.

```
(not CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"EQ","true"),nil,"The required hotfix is not installed on your PC."))
```

or you could define it this way (which makes more sense):

```
(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"),"The required hotfix is not installed on your PC.",nil))
```

You can build the expression in this example because the debug dap trace returns:

```
endpoint.os.windows.hotfix["KB923414"] = "true";
```

### Checking for Antivirus Programs

You can configure messages so that the end user is aware of and able to fix problems with missing or not running AVs. As a result, if access is denied, the security appliance collects all messages for the DAP that caused the "terminate" condition and displays them in the browser on the logon page. If access is allowed, the security appliance displays all messages generated in the process of DAP evaluation on the portal page.

The following instructions show how to use this feature to check on the Norton Antivirus program.

- 
- Step 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.av.NortonAV.exists, "EQ", "false"), "Your Norton AV was found but the active component of it was not enabled", nil) or
CheckAndMsg(EVAL(endpoint.av.NortonAV.exists, "NE", "true"), "Norton AV was not found on your computer", nil))
```

- Step 2** In that same Advanced field, select the **OR** button.

- Step 3** In the Access Attributes section below, set the leftmost tab, **Action**, to **Terminate**.

- Step 4** Connect from a PC that does not have or has disabled Norton Antivirus.

The expected result is that the connection is not allowed *and* the message appears as a blinking ! point.

- Step 5** Click the blinking ! to see the message.
- 

### Checking for Antivirus Programs and Definitions Older than 1 1/2 Days

This example checks for the presence of the Norton and McAfee antivirus programs, and whether the virus definitions are older than 1 1/2 days (10,000 seconds). If the definitions are older than 1 1/2 days, the security appliance terminates the session with a message and links for remediation.

- 
- Step 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).

```
((EVAL(endpoint.av.NortonAV.esists, "EQ", "true", "string") and
CheckAndMsg(EVAL(endpoint.av.NortonAV.lastupdate, "GT", "10000", integer"), To
remediate Click this link ", nil)) or
(EVAL(endpoint.av.McAfeeAV.esists, "EQ", "true", "string") and
CheckAndMsg(EVAL(endpoint.av.McAfeeAV.lastupdate, "GT", "10000", integer"), To
remediate Click this link", nil))
```

- Step 2** In that same Advanced field, select the **AND** button.

- Step 3** In the Access Attributes section below, set the leftmost tab, **Action**, to **Terminate**.

- Step 4** Connect from a PC that has Norton and McAfee antivirus programs with versions that are older than 1 1/2 days.

The expected result is that the connection is not allowed *and* the message appears as a blinking ! point.

**Step 5** Click the blinking ! to see the message and links for remediation.

---

## Advanced Lua Functions

When working with dynamic access policies for clientless SSL VPN, you might need additional flexibility of match criteria. For example, you might want to apply a different DAP based on the following:

- Organizational Unit (OU) or other level of the hierarchy for the user object
- Group Name that follows a naming convention but has many possible matches— you might require the ability to use a wildcard on group names.

You can accomplish this flexibility by creating a Lua logical expression in the Advanced section of the DAP pane in ASDM.

### OU-Based Match

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 on this criteria as follows:

```
(string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$" ~= nil)
```

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()
 if ((type(aaa.ldap.memberOf) == "string") and
 (string.find(aaa.ldap.memberOf, "-stu$" ~= nil)) then
 return true
 elseif (type(aaa.ldap.memberOf) == "table") then
 local k, v
 for k, v in pairs(aaa.ldap.memberOf) do
 if (string.find(v, "-stu$" ~= nil) then
 return true
 end
 end
 end
end
return false
```

```
end) ()
```

### Further Information on Lua

You can find detailed LUA programming information at <http://www.lua.org/manual/5.1/manual.html>.

## Operator for Endpoint Category

You can configure multiple instances of each type of endpoint. In this pane, set each type of endpoint to require only one instance of a type (Match Any = OR) or to have all instances of a type (Match All = AND).

- If you configure only one instance of an endpoint category, you do not need to set a value.
- For some endpoint attributes, it makes no sense to configure multiple instances. For example, no users have more than one running OS.
- You are configuring the Match Any/Match All operation within each endpoint type.

The security appliance evaluates each type of endpoint attribute, and then performs a logical AND operation on all of the configured endpoints. That is, each user must satisfy the conditions of ALL of the endpoints you configure, as well as the AAA attributes.

## DAP Examples

The following sections provide examples of useful dynamic access policies.

### Using 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 access. The policy named `Untrusted_VPN_Access` permits only clientless VPN access. [Table 36-4](#) summarizes the configuration of each of these policies.

The ASDM path is Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > Endpoint

**Table 36-4** A Simple DAP Configuration for Network Resources

| 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 and Web Portal   | Web Portal           |

## Using DAP to Apply a WebVPN ACL

DAP can directly enforce a subset of access policy attributes including Network ACLs (for IPsec and AnyConnect), clientless SSL VPN Web-Type ACLs, 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. You can define a DAP such that for a user in AD group (memberOf) = Engineering the security appliance applies a configured Web-Type ACL. To accomplish this task, perform the following steps:

- 
- Step 1** Navigate 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 menu to select 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 menu to select =, and in the adjacent text box 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 menu to select the ACL you want to apply to users in the AD group (memberOf) = Engineering.
- 

## Enforcing CSD Checks and Applying 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 security appliance. In addition, the security appliance 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.

- 
- Step 1** Navigate 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 menu to select 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 menu to select =, and in the adjacent text box 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 menu to select =, and in the adjacent text box enter Employees.
  - Step 7** For the AAA attribute type, use the drop-down menu to select Cisco.
  - Step 8** Check the Tunnel group box, use the drop-down menu to select =, and in the adjacent drop down box select the appropriate tunnel group (connection policy).
  - Step 9** In the Network ACL Filters tab of the Access Policy Attributes area, select the ACLs to apply to users who meet the DAP criteria defined in the previous steps.







# CHAPTER 37

## Clientless SSL VPN End User Set-up

This section is for the system administrator who sets up Clientless (browser-based) SSL VPN for end users. It summarizes configuration requirements and tasks for the user remote system. It also specifies information to communicate to users to get them started using Clientless SSL VPN. This section includes the following topics:

- [Requiring Usernames and Passwords](#)
- [Communicating Security Tips](#)
- [Configuring Remote Systems to Use Clientless SSL VPN Features](#)
- [Capturing Clientless SSL VPN Data](#)



### Note

We assume you have already configured the security appliance for Clientless SSL VPN.

## Requiring Usernames and Passwords

Depending on your network, during a remote session users might have to log in to any or all of the following: the computer itself, an Internet service provider, Clientless SSL VPN, mail or file servers, or corporate applications. Users might have to authenticate in many different contexts, requiring different information, such as a unique username, password, or PIN.

[Table 37-1](#) lists the type of usernames and passwords that Clientless SSL VPN users might need to know.

**Table 37-1**      *Usernames and Passwords to Give to Clientless SSL VPN Users*

| Login Username/<br>Password Type | Purpose                                          | Entered When                                                                              |
|----------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------|
| Computer                         | Access the computer                              | Starting the computer                                                                     |
| Internet Service Provider        | Access the Internet                              | Connecting to an Internet service provider                                                |
| Clientless SSL VPN               | Access remote network                            | Starting a Clientless SSL VPN session                                                     |
| File Server                      | Access remote file server                        | Using the Clientless SSL VPN file browsing feature to access a remote file server         |
| Corporate Application Login      | Access firewall-protected internal server        | Using the Clientless SSL VPN web browsing feature to access an internal protected website |
| Mail Server                      | Access remote mail server via Clientless SSL VPN | Sending or receiving e-mail messages                                                      |



## Communicating Security Tips

Advise users always to log out from the session. (To log out of Clientless SSL VPN, click the logout icon on the Clientless SSL VPN toolbar or close the browser.)

Advise users that using Clientless SSL VPN does not ensure that communication with every site is secure. Clientless SSL VPN ensures the security of data transmission between the remote PC or workstation and the security appliance 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 security appliance to the destination web server is not secure.

## Configuring Remote Systems to Use Clientless SSL VPN Features

[Table 37-2](#) includes the following information about setting up remote systems to use Clientless SSL VPN:

- Starting Clientless SSL VPN
- Using the Clientless SSL VPN Floating Toolbar
- Web Browsing
- Network Browsing and File Management
- Using Applications (Port Forwarding)
- Using E-mail via Port Forwarding
- Using E-mail via Web Access
- Using E-mail via e-mail proxy

[Table 37-2](#) also provides information about the following:


- Clientless SSL VPN requirements, by feature
- Clientless SSL VPN supported applications
- Client application installation and configuration requirements
- Information you might need to provide end users
- Tips and use suggestions for end users

It is possible you have configured user accounts differently and that different features are available to each Clientless SSL VPN user. [Table 37-2](#) organizes information by feature, so you can skip over the information for unavailable features.

**Table 37-2**      **Clientless SSL VPN Remote System Configuration and End User Requirements**

| Task                        | Remote System or End User Requirements   | Specifications or Use Suggestions                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Starting Clientless SSL VPN | Connection to the Internet               | Any Internet connection is supported, including: <ul style="list-style-type: none"> <li>• Home DSL, cable, or dial-ups</li> <li>• Public kiosks</li> <li>• Hotel hook-ups</li> <li>• Airport wireless nodes</li> <li>• Internet cafes</li> </ul>                                                                                                                                                                                                             |
|                             | Clientless SSL VPN-supported browser     | We recommend the following browsers for Clientless SSL VPN. Other browsers might not fully support Clientless SSL VPN features.<br>On Microsoft Windows: <ul style="list-style-type: none"> <li>• Internet Explorer version 6.0</li> <li>• Firefox 1.x</li> </ul> On Linux: <ul style="list-style-type: none"> <li>• Firefox 1.x</li> </ul> On Macintosh OS X: <ul style="list-style-type: none"> <li>• Safari version 1.0</li> <li>• Firefox 1.x</li> </ul> |
|                             | Cookies enabled on browser               | Cookies must be enabled on the browser in order to access applications via port forwarding.                                                                                                                                                                                                                                                                                                                                                                  |
|                             | URL for Clientless SSL VPN               | An https address in the following form:<br><code>https://address</code><br>where <i>address</i> is the IP address or DNS hostname of an interface of the security appliance (or load balancing cluster) on which Clientless SSL VPN is enabled. For example: <code>https://10.89.192.163</code> or <code>https://cisco.example.com</code> .                                                                                                                  |
|                             | Clientless SSL VPN username and password |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                             | [Optional] Local printer                 | Clientless SSL VPN does not support printing from a web browser to a network printer. Printing to a local printer is supported.                                                                                                                                                                                                                                                                                                                              |


Table 37-2 Clientless SSL VPN Remote System Configuration and End User Requirements (continued)

| Task                                                          | Remote System or End User Requirements               | Specifications or Use Suggestions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Using the Floating Toolbar in a Clientless SSL VPN Connection |                                                      | <p>A floating toolbar is available to simplify the use of Clientless SSL VPN. The toolbar lets you enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.</p> <p>If you configure your browser to block popups, the floating toolbar cannot display.</p> <p>The floating toolbar represents the current Clientless SSL VPN session. If you click the <b>Close</b> button, the security appliance prompts you to confirm that you want to close the Clientless SSL VPN session.</p> <p> <b>Tip</b> TIP: To paste text into a text field, use Ctrl-V. (Right-clicking is disabled on the Clientless SSL VPN toolbar.)</p>                                                                                                                                                                                                                                                              |
| Web Browsing                                                  | <p>Username and passwords for protected websites</p> | <p>Using Clientless SSL VPN does not ensure that communication with every site is secure. See <a href="#">“Communicating Security Tips.”</a></p> <p>The look and feel of web browsing with Clientless SSL VPN might be different from what users are accustomed to. For example:</p> <ul style="list-style-type: none"> <li>• The Clientless SSL VPN title bar appears above each web page.</li> <li>• You access websites by: <ul style="list-style-type: none"> <li>– Entering the URL in the Enter Web Address field on the Clientless SSL VPN Home page.</li> <li>– Clicking on a preconfigured website link on the Clientless SSL VPN Home page.</li> <li>– Clicking a link on a webpage accessed via one of the previous two methods.</li> </ul> </li> </ul> <p>Also, depending on how you configured a particular account, it might be that:</p> <ul style="list-style-type: none"> <li>• Some websites are blocked.</li> <li>• Only the web sites that appear as links on the Clientless SSL VPN Home page are available.</li> </ul> |

**Table 37-2** *Clientless SSL VPN Remote System Configuration and End User Requirements (continued)*

| Task                                        | Remote System or End User Requirements                             | Specifications or Use Suggestions                                                                                                                                                                              |
|---------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Browsing and File Management</b> | File permissions configured for shared remote access               | Only shared folders and files are accessible via Clientless SSL VPN.                                                                                                                                           |
|                                             | Server name and passwords for protected file servers               | —                                                                                                                                                                                                              |
|                                             | Domain, workgroup, and server names where folders and files reside | Users might not be familiar with how to locate their files through your organization network.                                                                                                                  |
|                                             | —                                                                  | Do not interrupt the <b>Copy File to Server</b> command or navigate to a different screen while the copying is in progress. Interrupting the operation can cause an incomplete file to be saved on the server. |

Table 37-2 Clientless SSL VPN Remote System Configuration and End User Requirements (continued)

| Task                                                                 | Remote System or End User Requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Specifications or Use Suggestions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Using Applications<br>(called Port Forwarding or Application Access) | <b>Note</b> On Macintosh OS X, only the Safari browser supports this feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                      | <b>Note</b> Because this feature requires installing Sun Microsystems Java™ Runtime Environment and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                      |  <b>Caution</b> Users should always close the Application Access window when they finish using applications by clicking the <b>Close</b> icon. Failure to quit the window properly can cause Application Access or the applications themselves to be disabled.                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                                      | Client applications installed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                                                      | Cookies enabled on browser                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                                                      | Administrator privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | User must have administrator access on the PC if you use DNS names to specify servers because modifying the hosts file requires it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                                      | Sun Microsystems Java Runtime Environment (JRE) version 1.4.x and 1.5.x installed.<br><br>Javascript must be enabled on the browser. By default, it is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                    | If JRE is not installed, a pop-up window displays, directing users to a site where it is available.<br><br>On rare occasions, the port forwarding applet fails with JAVA exception errors. If this happens, do the following:<br><br><ol style="list-style-type: none"> <li>1. Clear the browser cache and close the browser.</li> <li>2. Verify that no JAVA icons are in the computer task bar. Close all instances of JAVA.</li> <li>3. Establish a Clientless SSL VPN session and launch the port forwarding JAVA applet.</li> </ol>                                                                                                                                |
|                                                                      | Client applications configured, if necessary.<br><br><b>Note</b> The Microsoft Outlook client does not require this configuration step.<br><br>All non-Windows client applications require configuration.<br><br>To see if configuration is necessary for a Windows application, check the value of the Remote Server.<br><br><ul style="list-style-type: none"> <li>• If the Remote Server contains the server hostname, you do not need to configure the client application.</li> <li>• If the Remote Server field contains an IP address, you must configure the client application.</li> </ul> | To configure the client application, use the server's locally mapped IP address and port number. To find this information:<br><br><ol style="list-style-type: none"> <li>1. Start Clientless SSL VPN on the remote system and click the Application Access link on the Clientless SSL VPN Home page. The Application Access window appears.</li> <li>2. In the Name column, find the name of the server you want to use, then identify its corresponding client IP address and port number (in the Local column).</li> <li>3. Use this IP address and port number to configure the client application. Configuration steps vary for each client application.</li> </ol> |
|                                                                      | <b>Note</b> Clicking a URL (such as one in an -e-mail message) in an application running over Clientless SSL VPN does not open the site over Clientless SSL VPN. To open a site over Clientless SSL VPN, cut and paste the URL into the Enter (URL) Address field.                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 37-2** Clientless SSL VPN Remote System Configuration and End User Requirements (continued)

| Task                                | Remote System or End User Requirements                                                                                                                                                                                   | Specifications or Use Suggestions                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Using E-mail via Application Access | Fulfill requirements for Application Access (See Using Applications)                                                                                                                                                     | To use mail, start Application Access from the Clientless SSL VPN Home page. The mail client is then available for use.                                                                                                                                                                                                                             |
|                                     | <p><b>Note</b> If you are using an IMAP client and you lose your mail server connection or are unable to make a new connection, close the IMAP application and restart Clientless SSL VPN.</p> <p>Other mail clients</p> | <p>We have tested Microsoft Outlook Express versions 5.5 and 6.0.</p> <p>Clientless SSL VPN should support other SMTPS, POP3S, or IMAP4S e-mail programs via port forwarding, such as Lotus Notes, and Eudora, but we have not verified them.</p>                                                                                                   |
| Using E-mail via Web Access         | Web-based e-mail product installed                                                                                                                                                                                       | <p>Supported products include:</p> <ul style="list-style-type: none"> <li>Outlook Web Access</li> </ul> <p>For best results, use OWA on Internet Explorer 6.x or higher, or Firefox 1.x.</p> <ul style="list-style-type: none"> <li>Lotus iNotes</li> </ul> <p>Other web-based e-mail products should also work, but we have not verified them.</p> |
| Using E-mail via E-mail Proxy       | <p>SSL-enabled mail application installed</p> <p>Do not set the security appliance SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.</p>                                                        | <p>Supported mail applications:</p> <ul style="list-style-type: none"> <li>Microsoft Outlook</li> <li>Microsoft Outlook Express versions 5.5 and 6.0</li> <li>Eudora 4.2 for Windows 2000</li> </ul> <p>Other SSL-enabled mail clients should also work, but we have not verified them.</p>                                                         |
|                                     | Mail application configured                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                     |

## Capturing Clientless SSL VPN Data

The CLI capture command lets you log information about websites that do not display properly over a Clientless SSL VPN connection. This data can help your Cisco customer support engineer troubleshoot problems. The following sections describe how to use the capture command:

- [Creating a Capture File](#)
- [Using a Browser to Display Capture Data](#)



### Note

Enabling Clientless SSL VPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files needed for troubleshooting.

## Creating a Capture File

Perform the following steps to capture data about a Clientless SSL VPN session to a file.

- 
- Step 1** To start the Clientless SSL VPN capture utility, use the **capture** command from privileged EXEC mode.
- ```
capture capture_name type webvpn user webvpn_username
```
- where:
- *capture_name* is a name you assign to the capture, which is also prepended to the name of the capture files.
 - *webvpn_user* is the username to match for capture.
- The capture utility starts.
- Step 2** A user logs in to begin a Clientless SSL VPN session. The capture utility is capturing packets.
- Stop the capture by using the **no** version of the command.
- ```
no capture capture_name
```
- The capture utility creates a *capture\_name.zip* file, which is encrypted with the password **koleso**.
- Step 3** Send the .zip file to Cisco Systems, or attach it to a Cisco TAC service request.
- Step 4** To look at the contents of the .zip file, unzip it using the password **koleso**.
- 

The following example creates a capture named *hr*, which captures Clientless SSL VPN traffic for user2 to a file:

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
 capture name hr
 user name user2
hostname# no capture hr
```

## Using a Browser to Display Capture Data

Perform the following steps to capture data about a Clientless SSL VPN session and view it in a browser.

- 
- Step 1** To start the Clientless SSL VPN capture utility, use the **capture** command from privileged EXEC mode.
- ```
capture capture_name type webvpn user webvpn_username
```
- where:
- *capture_name* is a name you assign to the capture, which is also prepended to the name of the capture files.
 - *webvpn_username* is the username to match for capture.
- The capture utility starts.
- Step 2** A user logs in to begin a Clientless SSL VPN session. The capture utility is capturing packets.
- Stop the capture by using the **no** version of the command.
- Step 3** Open a browser and in the address box enter

`https://IP_address or hostname of the security appliance/webvpn_capture.html`

The captured content displays in a sniffer format.

- Step 4** When you finish examining the capture content, stop the capture by using the **no** version of the command.
-



CHAPTER 38

Clientless SSL VPN

Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. Clientless SSL VPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS Internet sites. Clientless SSL VPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to Clientless SSL VPN resources on a user or group basis. Users have no direct access to resources on the internal network.

Clientless SSL VPN works on the platform in single, routed mode.

For information on configuring Clientless SSL VPN for end users, see [Clientless SSL VPN End User Set-up](#).

Security Precautions

Clientless SSL VPN connections on the security appliance are very different from remote access IPSec connections, particularly with respect to how they interact with SSL-enabled servers, and precautions to reduce security risks.

In a Clientless SSL VPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a user of Clientless SSL VPN connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate.

The current implementation of Clientless SSL VPN does not permit communication with sites that present expired certificates. Nor does the security appliance perform trusted CA certificate validation. Therefore, users of Clientless SSL VPN cannot analyze the certificate an SSL-enabled web server presents before communicating with it.

To minimize the risks involved with SSL certificates:

- Configure a group policy for all users who need Clientless SSL VPN access, and enable Clientless SSL VPN only for that group policy.
- Limit Internet access for users of Clientless SSL VPN. One way to do this is to clear the **Enable URL entry** check box on the Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies panel, Functions tab. Then configure links to specific targets within the private network (Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies panel, URL Lists tab).

- Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a Clientless SSL VPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

ACLs

You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers.

- If you do not define any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic.

This pane lets you add and edit ACLs to be used for Clientless SSL VPN sessions, and the ACL entries each ACL contains. It also displays summary information about ACLs and ACEs, and lets you enable or disable them, and change their priority order.

Fields

- Add ACL—Click to add an ACL or ACE. To insert a new ACE before or after an existing ACE, click Insert or Insert After.
- Edit—Click to edit the highlighted ACE. When you delete an ACL, you also delete all of its ACEs. No warning or undelete.
- Delete—Click to delete the highlighted ACL or ACE. When you delete an ACL, you also delete all of its ACEs. No warning or undelete.
- Move UP/Move Down—Highlight an ACL or ACE and click these buttons to change the order of ACLs and ACEs. The security appliance checks ACLs to be applied to Clientless SSL VPN sessions and their ACEs in the sequence determined by their position in the ACLs list box until it finds a match.
- +/-—Click to expand (+) or collapse (-) to view or hide the list of ACEs under each ACL.
- No—Displays the priority of the ACEs under each ACL. The order in the list determines priority.
- Enabled—Shows whether the ACE is enabled. When you create an ACE, by default it is enabled. Clear the check box to disable an ACE.
- Address—Displays the IP address or URL of the application or service to which the ACE applies.
- Service—Displays the TCP service to which the ACE applies.
- Action—Displays whether the ACE permits or denies Clientless SSL VPN access.
- Time—Displays the time range associated with the ACE.
- Logging (Interval)—Displays the configured logging behavior, either disabled or with a specified level and time interval.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add ACL

This pane lets you create a new ACL.

Fields

- ACL Name—Enter a name for the ACL. Maximum 55 characters.

Add/Edit ACE

An Access Control Entry permits or denies access to specific URLs and services. You can configure multiple ACEs for an ACL. ACLs apply ACEs in priority order, acting on the first match.

Fields

- Action—Permits or denies access to the specific networks, subnets, hosts, and web servers specified in the Filter group box.
- Filter—Specifies a URL or an IP address to which you want to apply the filter (permit or deny user access).
 - URL—Applies the filter to the specified URL.
 - Protocols (unlabeled)—Specifies the protocol part of the URL address.
 - ://x—Specifies the URL of the Web page to which to apply the filter.
 - TCP—Applies the filter to the specified IP address, subnet, and port.
 - IP Address—Specifies the IP address to which to apply the filter.
 - Netmask—Lists the standard subnet mask to apply to the address in the IP Address box.
 - Service—Identifies the service (such as https, kerberos, or any) to be matched. Displays a list of services from which you can select the service to display in the Service box.
 - 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.
- Rule Flow Diagram—Graphically depicts the traffic flow using this filter. This area might be hidden.
- Options—Specifies the logging rules. The default is Default Syslog.
 - Logging—Choose enable if you want to enable a specific logging level.
 - Syslog Level—Grayed out until you select Enable for the Logging attribute. Lets you select the type of syslog messages you want the security appliance to display.
 - Log Interval—Lets you select the number of seconds between log messages.
 - Time Range—Lets you select the name of a predefined time-range parameter set.
 - ...—Click to browse the configured time ranges or to add a new one.

Examples

Here are examples of ACLs for Clientless SSL VPN:

Action	Filter	Effect
Deny	url http://*.yahoo.com/	Denies access to all of Yahoo!
Deny	url cifs://fileserver/share/directory	Denies access to all files in the specified location.
Deny	url https://www.company.com/ directory/file.html	Denies access to the specified file.
Permit	url https://www.company.com/directory	Permits access to the specified location
Deny	url http://*:8080/	Denies HTTPS access to anywhere via port 8080.
Deny	url http://10.10.10.10	Denies HTTP access to 10.10.10.10.
Permit	url any	Permits access to any URL. Usually used after an ACL that denies url access.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring the Setup for Cisco Secure Desktop

The Cisco Secure Desktop Setup window displays the version and state of the Cisco Secure Desktop image if it is installed on the security appliance, indicates whether it is enabled, and shows the size of the cache used to hold the Cisco Secure Desktop and SSL VPN Client on the security appliance.

You can use the buttons in this window as follows:

- To transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device of the security appliance click **Upload**.
To prepare to install or upgrade Cisco Secure Desktop, use your Internet browser to download a securedesktop_asa_<n>_<n>*.pkg file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your PC. Then use this button to transfer a copy from your local computer to the flash device. Click **Browse Flash** to install it into the running configuration. Finally, check **Enable Secure Desktop**.
- To install or replace the Cisco Secure Desktop image on the flash device of the security appliance, click **Browse Flash**.

**Note**

If you click the **Browse Flash** button to upgrade or downgrade the Cisco Secure Desktop image, select the package to install, and click **OK**, the Uninstall Cisco Secure Desktop dialog window asks you if you want to delete the Cisco Secure Desktop distribution currently in the running configuration from the flash device. Click **Yes** if you want to save space on the flash device, or click **No** to reserve the option to revert to this version of Cisco Secure Desktop.

- To remove the Cisco Secure Desktop image and configuration file (sdesktop/data.xml) from the running configuration, click **Uninstall**.

If you click this button, the Uninstall Cisco Secure Desktop dialog window asks if you want to delete the Cisco Secure Desktop image that was named in the “Secure Desktop Image field” and all Cisco Secure Desktop data files (including the entire Cisco Secure Desktop configuration) from the flash device. Click **Yes** if you want to remove these files from both the running configuration and the flash device, or click **No** to remove them from the running configuration, but retain them on the flash device.

Fields

The Cisco Secure Desktop Setup pane displays the following fields:

- Secure Desktop Image—Displays the Cisco Secure Desktop image loaded into the running configuration. By default, the filename is in the format `securedesktop_asa_<n>_<n>*.pkg`. Click **Browse Flash** to insert or modify the value in this field.
- Enable Secure Desktop—Check and click **Apply** to do the following:
 - Make sure the file is a valid Cisco Secure Desktop image.
 - Create an “sdesktop” folder on disk0 if one is not already present.
 - Insert a data.xml (Cisco Secure Desktop configuration) file into the sdesktop folder if one is not already present.
 - Load the data.xml file into the running configuration.

**Note**

If you transfer or replace the data.xml file, disable and then enable Cisco Secure Desktop to load the file.

- Enable Cisco Secure Desktop.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload Image

The Upload Image dialog box lets you transfer a copy of a Cisco Secure Desktop image from your local computer to the flash device on the security appliance. Use this window to install or upgrade Cisco Secure Desktop.



Note

Before using this window, use your Internet browser to download a `securedesktop_asa_<n>_<n>*.pkg` file from <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop> to any location on your local computer.

You can use the buttons in this window as follows:

- To select the path of the `securedesktop_asa_<n>_<n>*.pkg` file to be transferred, click **Browse Local Files**. The Selected File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the `securedesktop_asa_<n>_<n>*.pkg` file, select it, and click **Open**.
- To select the target directory for the file, click **Browse Flash**. The Browse Flash dialog box displays the contents of the flash card.
- To upload the `securedesktop_asa_<n>_<n>*.pkg` file from your local computer to the flash device, click **Upload File**. A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog window removes the contents of the Local File Path and Flash File System Path fields.
- To close the Upload Image dialog window, click **Close**. Click this button after you upload the Cisco Secure Desktop image to the flash device or if you decide not to upload it. If you uploaded it, the filename appears in the Secure Desktop Image field of the Cisco Secure Desktop Setup window. If you did not upload it, a Close Message dialog box prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the Cisco Secure Desktop Setup pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

Fields

The Upload Image dialog box displays the following fields:

- **Local File Path**—Specifies the path to the `securedesktop_asa_<n>_<n>*.pkg` file on your local computer. Click **Browse Local** to automatically insert the path in this field, or enter the path. For example:
 D:\Documents and Settings\Windows_user_name.AMER\My Documents\My Downloads\securedesktop_asa_3_1_1_16.pkg
 ASDM inserts the file path into the Local File Path field.
- **Flash File System Path**—Specifies the destination path on the flash device of the security appliance and the name of the destination file. Click **Browse Flash** to automatically insert the path into this field, or enter the path. For example,
 disk0:/securedesktop_asa_3_1_1_16.pkg
- **File Name**—Located in the Browse Flash dialog box that opens if you click **Browse Flash**, this field displays the name of the Cisco Secure Desktop image you selected on your local computer. We recommend that you use this name to prevent confusion. Confirm that this field displays the same name of the local file you selected and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path into the Flash File System Path field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Application Helper

Clientless SSL VPN includes an Application Profile Customization Framework option that lets the security appliance handle non-standard applications and web resources so they display correctly over a Clientless SSL VPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application. The script is in XML and uses sed (stream editor) syntax to transform strings/text.

Typically, Cisco TAC helps you write and apply an APCF.

You can configure multiple APCF profiles on a security appliance to run in parallel. Within an APCF profile script, multiple APCF rules can apply. In this case, the security appliance processes the oldest rule first, based on configuration history, the next oldest rule next, and so forth.

You can store APCF profiles on the security appliance flash memory, or on an HTTP, HTTPS, FTP, or TFTP server. Use this panel to add, edit, and delete APCF packages, and to put them in priority order.

Fields

- **APCF File Location**—Displays information about the location of the APCF package. This can be on the security appliance flash memory, or on an HTTP, HTTPS, FTP, or TFTP server.
- **Add/Edit**—Click to add or edit a new or existing APCF profile.
- **Delete**—Click to remove an existing APCF profile. There is no confirmation or undo.
- **Move Up**—Click to rearrange APCF profiles within a list. The list determines the order in which the security appliance attempts to use APCF profiles.

Add/Edit APCF Profile

This panel lets you add or edit an APCF package, which includes identifying its location, which can be either on the security appliance flash memory, or on an HTTP, HTTPS, or TFTP server.

Fields

- **Flash file**—Check to locate an APCF file stored on the security appliance flash memory.
- **Path**—Displays the path to an APCF file stored on flash memory after you browse to locate it. You can also manually enter the path in this field.
- **Browse Flash**—Click to browse flash memory to locate the APCF file. A Browse Flash Dialog panel displays. Use the Folders and Files columns to locate the APCF file. Highlight the APCF file and click **OK**. The path to the file then displays in the Path field.

**Note**

If you do not see the name of an APCF file that you recently downloaded, click the Refresh button.

- **Upload**—Click to upload an APCF file from a local computer to the security appliance flash file system. The Upload APCF package pane displays.
- **URL**—Check to use an APCF file stored on an HTTP, HTTPS or TFTP server.
- **ftp, http, https, and tftp (unlabeled)**—Identify the server type.
- **URL (unlabeled)**—Enter the path to the FTP, HTTP, HTTPS, or TFTP server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload APCF package**Fields**

- **Local File Path**—Shows the path to the APCF file on your computer. Click **Browse Local** to automatically insert the path in this field, or enter the path.
- **Browse Local Files**—Click to locate and choose the APCF file on your computer that you want to transfer. The Select File Path dialog box displays the contents of the folder you last accessed on your local computer. Navigate to the APCF file, select it, and click **Open**. ASDM inserts the file path into the Local File Path field.
- **Flash File System Path**—Displays the path on the security appliance to upload the APCF file.
- **Browse Flash**—Click to identify the location on the security appliance to which you want to upload the APCF file. The Browse Flash dialog box displays the contents of flash memory.
- **File Name**—Located in the Browse Flash dialog box that opens when you click Browse Flash, this field displays the name of the APCF file you selected on your local computer. We recommend that you use this name to prevent confusion. Confirm that this file displays the correct filename, and click **OK**. The Browse Flash dialog box closes. ASDM inserts the destination file path in the Flash File System Path field.
- **Upload File**—Click when you have identified the location of the APCF file on your computer, and the location where you want to download it to the security appliance.
- A Status window appears and remains open for the duration of the file transfer. Following the transfer, an Information window displays the message, “File is uploaded to flash successfully.” Click **OK**. The Upload Image dialog window removes the contents of the Local File Path and Flash File System Path fields, indicating you can upload another file. To do so, repeat these instructions. Otherwise, click the **Close** button.
- **Close**—Closes the Upload Image dialog window. Click this button after you upload the APCF file to flash memory or if you decide not to upload it. If you do upload it, the filename appears in the APCF File Location field of the APCF window. If you do not upload it, a Close Message dialog box

prompts, “Are you sure you want to close the dialog without uploading the file?” Click **OK** if you do not want to upload the file. The Close Message and Upload Image dialog boxes close, revealing the APCF Add/Edit pane. Otherwise, click **Cancel** in the Close Message dialog box. The dialog box closes, revealing the Upload Image dialog box again, with the values in the fields intact. Click **Upload File**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Auto Signon

The Auto Signon window or tab lets you configure or edit auto signon for users of Clientless SSL VPN. Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. With auto signon configured for particular internal servers, the security appliance passes the login credentials that the user of Clientless SSL VPN entered to log in to the security appliance (username and password) to those particular internal servers. You configure the security appliance to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the security appliance to respond to consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these methods.

Auto signon is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto signon. If you already have SSO deployed using Computer Associates' SiteMinder SSO server, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO, and if you want to configure the security appliance to support this solution, see [SSO Servers](#).



Note

Do not enable auto signon for servers that do not require authentication or that use credentials different from the security appliance. When auto signon is enabled, the security appliance passes on the login credentials that the user entered to log into the security appliance regardless of what credentials are in user storage.

Fields

- **IP Address**—*Display only*. In conjunction with the following Mask, displays the IP address range of the servers to be authenticated to as configured with the Add/Edit Auto Signon dialog box. You can specify a server using either the server URI or the server IP address and mask.
- **Mask**—*Display only*. In conjunction with the preceding IP Address, displays the IP address range of the servers configured to support auto signon with the Add/Edit Auto Signon dialog box.
- **URI**—*Display only*. Displays a URI mask that identifies the servers configured with the Add/Edit Auto Signon dialog box.

- Authentication Type—*Display only*. Displays the type of authentication—Basic (HTTP), NTLM, FTP and CIFS, or all of these methods—as configured with the Add/Edit Auto Signon dialog box.
- Add/Edit—Click to add or edit an auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.
- Delete—Click to delete an auto signon instruction selected in the Auto Signon table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Auto Signon Entry

The Add/Edit Auto Signon Entry dialog box lets you add or edit a new auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.

Fields

- IP Block—Click this button to specify a range of internal servers using an IP address and mask.
 - IP Address—Enter the IP address of the first server in the range for which you are configuring auto sign-on.
 - Mask—In the subnet mask menu, click the subnet mask that defines the server address range of the servers supporting auto signon.
- URI—Click this button to specify a server supporting auto signon by URI, then enter the URI in the field next to this button.
- Authentication Type—The authentication method assigned to the servers. For the specified range of servers, the security appliance can be configured to respond to Basic HTTP authentication requests, NTLM authentication requests, FTP and CIFS authentication requests, or requests using any of these methods.
 - Basic—Click this button if the servers support basic (HTTP) authentication.
 - NTLM—Click this button if the servers support NTLMv1 authentication.
 - FTP/CIFS—Click this button if the servers support FTP and CIFS authentication
 - Basic, NTLM, and FTP/CIFS—Click this button if the servers support all of the above.



Note

If you configure one method for a range of servers (e.g., HTTP Basic) and one of those servers attempts to authenticate with a different method (e.g., NTLM), the security appliance does not pass the user login credentials to that server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Session Settings

The Clientless SSL VPN Add/Edit Internal Group Policy > More Options > Session Settings window lets you specify personalized user information between clientless SSL VPN sessions. By default, each group policy inherits the settings from the default group policy. Use this window to specify personalized clientless SSL VPN user information for the default group policy and any group policies for which you want to differentiate these values.

Fields

- User Storage Location—Choose none or choose the file server protocol (smb or ftp) from the drop-down menu. If you choose smb or ftp, use the following syntax to enter the file system destination into the adjacent text field:

username:password@host:port-number/path

For example

mike:mysecret@ftpserver3:2323/public



Note Although the configuration shows the username, password, and preshared key, the security appliance uses an internal algorithm to store the data in an encrypted form to safeguard it.

- Storage Key—Type the string, if required, for the security appliance to pass to provide user access to the storage location.
- Storage Objects—Select one of the following options from the drop-down menu to specify the objects the server uses in association with the user. The security appliance store these objects to support clientless SSL VPN connections.
 - cookies,credentials
 - cookies
 - credentials
- Transaction Size—Enter the limit in KB over which to time out the session. This attribute applies only to a single transaction. Only a transaction larger than this value resets the session expiration clock.

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Java Code Signer

Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.

To select a Java Code Signer, use the drop down list.

To configure a Java Code Signer, go to Configuration > Remote Access VPN > Certificate Management > Java Code Signer.

Content Cache

Caching enhances the performance of Clientless SSL VPN. It stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. The use of the cache reduces traffic, with the result that many applications run more efficiently.

Fields

- Enable cache—Check to enable caching. The default value is disable.
- Parameters—Lets you define the terms for caching.
 - Enable caching of compressed content—Check to cache compressed content. When you disable this parameter, the security appliance stores objects before it compresses them.
 - Maximum Object Size—Enter the maximum size in KB of a document that the security appliance can cache. The security appliance measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 1000 KB
 - Minimum Object Size—Enter the minimum size in KB of a document that the security appliance can cache. The security appliance measures the original content length of the object, not rewritten or compressed content. The range is 0 to 10,000 KB; the default is 0 KB.



Note

The Maximum Object Size must be greater than the Minimum Object Size.

- Expiration Time—Enter an integer between 0 and 900 to set the number of minutes to cache objects without revalidating them. The default is one minute.
- LM Factor—Enter an integer between 1 and 100; the default is 20.

The LM factor sets the policy for caching objects which have only the last-modified timestamp. This revalidates objects that have no server-set change values. The security appliance estimates the length of time since the object has changed, also called the expiration time. The estimated expiration time equals the time elapsed since the last change multiplied by the LM factor. Setting the LM factor to 0 forces immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

The expiration time sets the amount of time to for the security appliance to cache objects that have neither a last-modified time stamp nor an explicit server-set expiry time.

- Cache static content—Click to cache all content that is not subject to rewrite, for example, PDF files and images.

- Restore Cache Default—Click to restore default values for all cache parameters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Content Rewrite

The Content Rewrite panel lists all applications for which content rewrite is enabled or disabled.

Clientless SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

You might not want some applications and web resources, for example, public websites, to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPsec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

Fields

- Content Rewrite
 - Rule Number—Displays an integer that indicates the position of the rule in the list.
 - Rule Name—Provides the name of the application for which the rule applies.
 - Rewrite Enabled—Displays content rewrite as enabled or disabled.
 - Resource Mask—Displays the resource mask.
- Add/Edit—Click to add a rewrite entry or edit a selected rewrite entry.
- Delete—Click to delete a selected rewrite entry.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Content Rewrite Rule

- Enable content rewrite—Check to enable content rewrite for this rewrite rule.
- Rule Number—(Optional) Enter a number for this rule. This number specifies the position of the rule in the list. Rules without a number are at the end of the list. The range is 1 to 65534.
- Rule Name—(Optional) Provide an alphanumeric string that describes the rule, maximum 128 characters.
- Resource Mask—Enter the resource mask. This is a word, length up to 300 characters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Java Code Signer

Java objects which have been transformed by Clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. In the Java Trustpoint pane, you can configure the Clientless SSL VPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location. To import a trustpoint, see Configuration > Properties > Certificate > Trustpoint > Import.

Fields

- Code Signer Certificate —Choose the configured certificate that you want to employ in Java object signing.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Encoding

This window lets you view or specify the character encoding for Clientless SSL VPN portal pages.

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0’s and 1’s) with characters to represent the data. The language determines the character encoding method to use. Some languages use a single method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the remote user can change it. The browser can also detect the encoding specified on the page, and render the document accordingly.

The encoding attribute lets you specify the value of the character-encoding method used on the portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, and regardless of any changes made to the browser.

By default, the security appliance applies the “Global Encoding Type” to pages from Common Internet File System servers. The mapping of CIFS servers to their appropriate character encoding, globally with the “Global Encoding Type” attribute, and individually with the file-encoding exceptions displayed in the table, provides for the accurate handling and display of CIFS pages when the proper rendering of filenames or directory paths, as well as pages, is an issue.

Fields

- **Global Encoding Type**—This attribute determines the character encoding that all Clientless SSL VPN portal pages inherit except for those from the CIFS servers listed in the table. You can type the string or select one of the options in the drop-down list, which contains the most common values, as follows:
 - big5
 - gb2312
 - ibm-850
 - iso-8859-1
 - shift_jis



Note If you are using Japanese Shift_jis Character encoding, click **Do not specify** in the Font Family area of the associated Select Page Font pane to remove the font family.

- unicode
- windows-1252
- none

If you choose **none** or specify a value that the browser on the Clientless SSL VPN session does not support, it uses its own default encoding.

You can type a string consisting of up to 40 characters, and equal to one of the valid character sets identified in <http://www.iana.org/assignments/character-sets>. You can use either the name or the alias of a character set listed on that page. The string is case-insensitive. The command interpreter converts upper-case to lower-case when you save the security appliance configuration.

- **CIFS Server**—Name or IP address of each CIFS server for which the encoding requirement differs from the “Global Encoding Type” attribute setting.

A difference in the encoding of the CIFS server filename and directory indicates that you might need to add an entry for the server to ensure the encoding is correct.

- **Encoding Type**—Displays the character encoding override for the associated CIFS server.
- **Add**—Click once for each CIFS server for which you want to override the “Global Encoding Type” setting.
- **Edit**—Select a CIFS server in the table and click this button to change its character encoding.

- Delete—Select a CIFS server in the table and click this button to delete the associated entry from the table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Encoding

The Add CIFS Server Encoding dialog window lets you maintain exceptions to the “Global Encoding Type” attribute setting in the Add CIFS Encoding window. That window contains the Add and Edit buttons that open this dialog box.

Fields

- CIFS Server—Enter the name or IP address of a CIFS server for which the encoding requirement differs from the “Global Encoding Type” attribute setting. The security appliance retains the case you specify, although it ignores the case when matching the name to a server.
- Encoding Type —Choose the character encoding that the CIFS server should provide for Clientless SSL VPN portal pages. You can type the string, or select one from the drop-down list, which contains only the most common values, as follows:
 - big5
 - gb2312
 - ibm-850
 - iso-8859-1
 - shift_jis



Note

If you are using Japanese Shift_jis Character encoding, click **Do not specify** in the Font Family area of the associated Select Page Font pane to remove the font family.

- unicode
- windows-1252
- none

If you choose **none** or specify a value that the browser on the Clientless SSL VPN session does not support, it uses its own default encoding.

You can type a string consisting of up to 40 characters, and equal to one of the valid character sets identified in <http://www.iana.org/assignments/character-sets>. You can use either the name or the alias of a character set listed on that page. The string is case-insensitive. The command interpreter converts upper-case to lower-case when you save the security appliance configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Web ACLs

The Web ACLs table displays the filters configured on the security appliance applicable to Clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the ACL name, the access control entries (ACEs) assigned to the ACL.

Each ACL permits or denies access permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL.

You can configure ACLs to apply to Clientless SSL VPN traffic. The following rules apply:

- If you do not configure any filters, all connections are permitted.
- The security appliance supports only an inbound ACL on an interface.
- At the end of each ACL, an implicit, unwritten rule denies all traffic that is not explicitly permitted.

You can add ACLs and ACEs as follows:

- To add an ACL, click the down arrow next to the plus sign above the table and click **Add ACL**.



Note An ACL must be present before you can add an ACE.

- To add an ACE to an ACL that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Add ACE**.
- To insert an ACE before an ACE that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Insert**.
- To insert an ACE after an ACE that is already present in the table, select it, then click the down arrow next to the plus sign above the table and click **Insert After**.

To change the values assigned to an ACE, double-click it, or select it and click **Edit**.

To remove an ACL or an ACE, select the entry in the table and click **Delete**.

The relative position of an ACE in an ACL determines the sequence with which the security appliance applies it to traffic on the interface. You can reorganize and reuse the ACEs present in the table as follows.

- To move an ACE above or below another ACE, select it and click the up or down icon above the table.
- To move an ACE, select the ACE, click the scissors icon above the table. Select the target ACL or ACE, click the arrow next to the clipboard icon, and click **Paste** to paste above the selection or **Paste After** to paste after the selection. The Edit ACE window opens, providing you with an opportunity to change the values. Click **OK**.
- To copy an ACE, select it and click the double-page icon above the table. Select the target ACL or ACE, click the arrow next to the clipboard icon, and click **Paste** to paste above the selection or **Paste After** to paste after the selection. The Edit ACE window opens, providing you with an opportunity to change the values. Click **OK**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Port Forwarding

Both the Port Forwarding pane and Configure Port Forwarding Lists dialog box let you view the port forwarding lists. Both the Port Forwarding pane and the Add or Edit Port Forwarding Entry dialog box let you specify the name of a port forwarding list, and add, view, edit, and delete port forwarding entries to the list.

To add, change, or remove a port forwarding list, do one of the following:

- To add a port forwarding list and add entries to it, choose **Add**. The Add Port Forwarding List dialog box opens. After you name the list, click **Add** again. ASDM opens the Add Port Forwarding Entry dialog box, which lets you assign the attributes of an entry to the list. After doing so and clicking OK, ASDM displays those attributes in the list. Repeat as needed to complete the list, then click **OK** in the Add Port Forwarding List dialog box.
- To change a port forwarding list, double-click the list or select the list in the table and click **Edit**. Then click **Add** to insert a new entry into the list, or select an entry in the list and click **Edit** or **Delete**.
- To remove a list, select the list in the table and click **Delete**.

The following sections describe port forwarding and how to configure it:

- [Port Forwarding Capabilities and Restrictions](#)
- [Add/Edit Port Forwarding List](#)
- [Add/Edit Port Forwarding Entry](#)

Port Forwarding Capabilities and Restrictions

Port forwarding lets users access TCP-based applications over a Clientless SSL VPN connection. Such applications include the following:

Lotus Notes	Secure FTP (FTP over SSH)
Outlook Express	SSH
Outlook	TELNET
Perforce	Windows Terminal Service
Sametime	XDDTS

Other TCP-based applications may also work, but we have not tested them. Protocols that use UDP do not work.

The following restrictions apply to port forwarding:

- The remote host must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000.
- Users of Microsoft Windows Vista who use port forwarding or smart tunnels must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.
- Port forwarding supports only TCP applications that use static TCP ports. Applications that use dynamic ports or multiple TCP ports are not supported. For example, SecureFTP, which uses port 22, works over clientless SSL VPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.
- The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. Neither port forwarding nor the smart tunnel feature supports MAPI. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.
- A stateful failover does not retain sessions established using Application Access (either port forwarding or smart tunnel access). Users must reconnect following a failover.
- Port forwarding does not support connections to personal digital assistants.
- Because port forwarding requires downloading the Java applet and configuring the local client, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.

**Caution**

Make sure Sun Microsystems Java™ Runtime Environment (JRE) 1.5.x is installed on the remote computers to support port forwarding (application access) and digital certificates. If JRE 1.4.x is running and the user authenticates with a digital certificate, the application fails to start because JRE cannot access the web browser's certificate store.

The Java applet displays in its own window on the end user HTML interface. It shows the contents of the list of forwarded ports available to the user, as well as which ports are active, and amount of traffic in bytes sent and received.

- Neither port forwarding nor the ASDM Java applet work with user authentication using digital certificates. Java does not have the ability to access the web browser keystore. Therefore Java cannot use certificates that the browser uses to authenticate users, and the application cannot start.

Add/Edit Port Forwarding List

The Add/Edit Port Forwarding List dialog boxes let you add or edit a named list of TCP applications to associate with users or group policies for access over clientless SSL VPN connections.

Fields

- List Name—Alpha-numeric name for the list. Maximum 64 characters.
- Local TCP Port—Local port that listens for traffic for the application.
- Remote Server—IP address or DNS name of the remote server.
- Remote TCP Port—Remote port that listens for traffic for the application.
- Description—Text that describes the TCP application.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Port Forwarding Entry

The Add/Edit Port Forwarding Entry dialog boxes let you specify TCP applications to associate with users or group policies for access over clientless SSL VPN connections. Assign values to the attributes in these windows as follows:

- **Local TCP Port**—Type a TCP port number for the application to use. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.
- **Remote Server**—Type either the DNS name or IP address of the remote server. We recommend using hostnames so that you do not have to configure the client applications for specific IP addresses.
- **Remote TCP Port**—Type the well-know port number for the application.
- **Description**—Type a description of the application. Maximum 64 characters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring the Use of External Proxy Servers

Use the Proxies pane to configure the security appliance to use external proxy servers to handle HTTP requests and HTTPS requests. These servers act as an intermediary between users and the Internet. Requiring all Internet access via servers you control provides another opportunity for filtering to assure secure Internet access and administrative control.



Note

HTTP and HTTPS proxy services do not support connections to personal digital assistants.

Fields

Use an HTTP proxy server—Click to use an external HTTP proxy server.

- **Specify IP address of proxy server**—Click to identify the HTTP proxy server by its IP address or hostname.
- **IP Address**—Enter the hostname or IP address of the external HTTP proxy server
- **Port**—Enter the port that listens for HTTP requests. The default port is 80.

- **Exception Address List— (Optional)** Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTP proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:
 - * to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
 - ? to match any single character, including slashes and periods.
 - [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.
 - [!x-y] to match any single character that is not in the range.
- **UserName—(Optional)** Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
- **Password—**Enter a password to send to the proxy server with each HTTP request.
- **Specify PAC file URL—**As an alternative to specifying the IP address of the HTTP proxy server, you can click this option to specify a Proxy autoconfiguration file to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL. Enter **http://** and type the URL of the proxy autoconfiguration file into the adjacent field. If you omit the **http://** portion, the security appliance ignores it.

Use an HTTPS proxy server—Click to use an external HTTPS proxy server.

- **Specify IP address of proxy server—**Click to identify the HTTPS proxy server by its IP address or hostname.
- **IP Address—**Enter the hostname or IP address of the external HTTPS proxy server
- **Port—**Enter the port that listens for HTTPS requests. The default port is 443.
- **Exception Address List— (Optional)** Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTPS proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:
 - * to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
 - ? to match any single character, including slashes and periods.
 - [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.
 - [!x-y] to match any single character that is not in the range.
- **UserName—(Optional)** Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
- **Password—**Enter a password to send to the proxy server with each HTTPS request.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Proxy Bypass

You can configure the security appliance to use proxy bypass when applications and web resources work better with the special content rewriting this feature provides. Proxy bypass is an alternative method of content rewriting that makes minimal changes to the original content. It is often useful with custom web applications.

You can configure multiple proxy bypass entries. The order in which you configure them is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the security appliance. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is the text in a URL that follows the domain name. For example, in the URL `www.mycompany.com/hrbenefits`, *hrbenefits* is the path. Similarly, for the URL `www.mycompany.com/hrinsurance`, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: `/hr*`.

Fields

- Interface—Displays the VLAN configured for proxy bypass.
- Port—Displays the port configured for proxy bypass.
- Path Mask—Displays the URI path to match for proxy bypass.
- URL—Displays the target URLs.
- Rewrite—Displays the rewrite options. These are a combination of XML, link, or none.
- Add/Edit—Click to add a proxy bypass entry or edit a selected entry.
- Delete—Click to delete a proxy bypass entry.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Proxy Bypass Rule

This panel lets you set rules for when the security appliance performs little or no content rewriting.

Fields

- Interface Name—Select the VLAN for proxy bypass.
- Bypass Condition—Specify either a port or a URI for proxy bypass.
 - Port—(radio button) Click to use a port for proxy bypass. The valid port numbers are 20000-21000.
 - Port (field)—Enter a high-numbered port for the security appliance to reserve for proxy bypass.
 - Path Mask—(radio button) Click to use a URL for proxy bypass.
 - Path Mask—(Field) Enter a URL for proxy bypass. It can contain a regular expression.
- URL—Define target URLs for proxy bypass.
 - URL—(drop-down list) Select either http or https as the protocol.
 - URL (text field)—Enter a URL to which you want to apply proxy bypass.
- Content to Rewrite—Specifies the content to rewrite. The choices are none or a combination of XML, links, and cookies.
 - XML—Check to rewrite XML content.
 - Hostname—Check to rewrite links.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

DTLS Settings

Enabling Datagram Transport Layer Security (DTLS) allows the AnyConnect VPN 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 some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL VPN tunnel only.

Fields

- Interface—Displays a list of interfaces on the security appliance.
- DTLS Enabled—Check to enable DTLS connections with the AnyConnect client on the interfaces.
- UDP Port (default 443)—(Optional) Specify a separate UDP port for DTLS connections.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SSL VPN Client Settings

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. The client gives remote users the benefits of an SSL VPN client without the need for network administrators to install and configure clients on remote computers.

Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The security appliance downloads the client based on the group policy or local user policy attributes. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

Fields

- **SSL VPN Client Images table**—Displays the package files specified as SSL VPN client images, and allows you to establish the order that the security appliance downloads the images to the remote PC.
 - **Add**—Displays the Add SSL VPN Client Image window, where you can specify a file in flash memory as a client image file, or where 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 SSL VPN Client Image window, 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—changes the order in which the security appliance 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.
- SSL VPN Client Profiles table—Displays the XML files specified as SSL VPN client profiles. These profiles display host information in the AnyConnect VPN Client user interface.
 - Add—Displays the Add SSL VPN Client Profiles window, 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.
 - Edit—Displays the Edit SSL VPN Client Profiles window, where you can specify a file in flash memory as a profile to replace a profile highlighted in the SSL VPN Client Profiles table. You can also upload a file from a local computer to the flash memory.
 - Delete—Deletes a profile from the table. This does not delete the XML file from flash.
- Cache File System—The security appliance expands SSL VPN client and CSD images in cache memory. Adjust the size of cache memory to ensure the images have enough space to expand.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

For More Information

Add/Replace SSL VPN Client Image

In this window, you can specify a filename for a file on the security appliance flash memory that you want to add as an SSL VPN 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.

Fields

- 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 window where you can view all the files on flash memory.
- Upload—Displays the Upload Image window 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 security appliance 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 security appliance, it includes the User-Agent string in the HTTP header. When the security appliance receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload Image

In this window, 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 SSL VPN client image. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

Fields

- 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 window where you can view all the files on local computer and where you can select 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 window where you can view all the files on flash memory of the security appliance and where you can select a file to identify as a client image.
- Upload File—Initiates the file upload.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit SSL VPN Client Profiles

In this window, 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 SSL VPN client profile. These profiles display host information in the AnyConnect VPN Client user interface. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

Fields

- Profile Name—Associates a name with the XML file that appears in the table. Provide any name that makes it easy for you to remember the hosts identified in the XML profile file.

- **Profile Package**—Identifies the filename of the file in flash memory on the local computer that you want to identify as an SSL VPN client profile.
- **Browse Flash**—Displays the Browse Flash Dialog window where you can view all the files on flash memory of the security appliance and where you can select a file to identify as a profile.
- **Upload File**—Initiates the file upload.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Upload Package

In this window, 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 SSL VPN client profile. You can also browse the local computer or the flash memory of the security appliance for a file to identify.

Fields

- **Local File Path**—Identifies the filename of the file in on the local computer that you want to identify as an SSL VPN client profile.
- **Browse Local Files**—Displays the Select File Path window where you can view all the files on local computer and where you can select a file to identify as a client profile.
- **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 client profile.
- **Browse Flash**—Displays the Browse Flash Dialog window where you can view all the files on flash memory of the security appliance and where you can select a file to identify as a client profile.
- **Upload File**—Initiates the file upload.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Bypass Interface Access List

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.

- Enable inbound IPSec sessions to bypass interface access-lists. Group policy and per-user authorization access lists still apply to the traffic—By default, the security appliance allows VPN traffic to terminate on a security appliance 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 security appliance performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.)

SSO Servers

The SSO Server window lets you configure or delete single sign-on (SSO) for users of Clientless SSL VPN connecting to a Computer Associates SiteMinder SSO server or to a Security Assertion Markup Language (SAML), Version 1.1, Browser Post Profile SSO server. SSO support, available only for Clientless SSL VPN, lets users access different secure services on different servers without entering a username and password more than once.

You can choose from four methods when configuring SSO: Auto Signon using basic HTTP and/or NTLMv1 authentication, HTTP Form protocol, or Computer Associates eTrust SiteMinder (formerly Netegrity SiteMinder), or SAML, Version 1.1 Browser Post Profile.

**Note**

The SAML Browser Artifact profile method of exchanging assertions is not supported.

This section describes the procedures for setting up SSO with both SiteMinder and SAML Browser Post Profile.

- To configure SSO with basic HTTP or NTLM authentication, see [Auto Signon](#).
- To configure SSO with the HTTP Form protocol, see [Configuring Session Settings](#).

The SSO mechanism either starts as part of the AAA process (HTTP Forms) or just after successful user authentication to either a AAA server (SiteMinder) or a SAML Browser Post Profile server. In these cases, the Clientless SSL VPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the Clientless SSL VPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS.

If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the Clientless SSL VPN server. This cookie is kept on the security appliance on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

Configuring SiteMinder and SAML Browser Post Profile

SSO authentication with SiteMinder or with SAML Browser Post Profile is separate from AAA and occurs after the AAA process completes. To set up SiteMinder SSO for a user or group, you must first configure a AAA server (RADIUS, LDAP and so forth). After the AAA server authenticates the user, the Clientless SSL VPN server uses HTTPS to send an authentication request to the SiteMinder SSO server.

In addition to configuring the security appliance, for SiteMinder SSO, you also must configure your CA SiteMinder Policy Server with the Cisco authentication scheme. See [Adding the Cisco Authentication Scheme to SiteMinder](#).

For SAML Browser Post Profile you must configure a Web Agent (Protected Resource URL) for authentication. For the specifics of setting up a SAML Browser Post Profile SSO server, see [SAML POST SSO Server Configuration](#).

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Signon Servers

Configure Single Signon (SSO) server parameters.
This parameter is enforced in either a VPN [user](#) or [group policy](#) configuration.

Server Name	Server Type	URL	Maximum Retries	Request Timeout (seconds)
sample	SAML POST		3	5
Sample	SAML POST		3	5

Buttons: Add, Edit, Delete, Apply, Reset

91700

Fields

- **Server Name**—*Display only*. Displays the names of configured SSO Servers. The minimum number of characters is 4, and the maximum is 31.
- **Authentication Type**—*Display only*. Displays the type of SSO server. The security appliance currently supports the SiteMinder type and the SAML Browser Post Profile type.

- **URL**—*Display only*. Displays the SSO server URL to which the security appliance makes SSO authentication requests.
- **Secret Key**—*Display only*. Displays the secret key used to encrypt authentication communications with the SSO server. The key can be comprised of any regular or shifted alphanumeric character. There is no minimum or maximum number of characters.
- **Maximum Retries**—*Display only*. Displays the number of times the security appliance retries a failed SSO authentication attempt. The range is 1 to 5 retries, and the default number of retries is 3.
- **Request Timeout (seconds)**—*Display only*. Displays the number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds, and the default number of seconds is 5.
- **Add/Edit**—Opens the Add/Edit SSO Server dialog box.
- **Delete**—Deletes the selected SSO server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SAML POST SSO Server Configuration

Use the SAML server documentation provided by the server software vendor to configure the SAML server in Relying Party mode. The following steps list the values required to configure the SAML Server for Browser Post Profile:

-
- Step 1** Configure the SAML server parameters to represent the asserting party (the security appliance):
- Recipient consumer (Web Agent) URL (same as the assertion consumer URL configured on the ASA)
 - Issuer ID, a string, usually the hostname of appliance
 - Profile type -Browser Post Profile
- Step 2** Configure certificates.
- Step 3** Specify that asserting party assertions must be signed.
- Step 4** Select how the SAML server identifies the user:
- Subject Name Type is DN
 - Subject Name format is uid=<user>

Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the security appliance for SSO with SiteMinder, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in.

**Note**

- Configuring the SiteMinder Policy Server requires experience with SiteMinder.
- This section presents general tasks, not a complete procedure.
- Refer to the CA SiteMinder documentation for the complete procedure for adding a custom authentication scheme.

To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform the following tasks:

- Step 1** With the Siteminder Administration utility, create a custom authentication scheme being sure to use the following specific arguments:
- In the Library field, enter **smjavaapi**.
 - In the Secret field, enter the same secret configured in the Secret Key field of the Add SSO Server dialog to follow.
 - In the Parameter field, enter **CiscoAuthApi**.
- Step 2** Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from <http://www.cisco.com/cgi-bin/tablebuild.pl/asa> and copy it to the default library directory for the SiteMinder server. This .jar file is also available on the Cisco security appliance CD.

Add/Edit SSO Servers

This SSO method uses CA SiteMinder and SAML Browser Post Profile. You can also set up SSO using the HTTP Form protocol, or Basic HTML and NTLM authentication. To use the HTTP Form protocol, see [Configuring Session Settings](#). To set use basic HTML or NTLM authentication, use the **auto-signon** command at the command line interface.

**Note**

1 91 702

Fields

- **Server Name**—If adding a server, enter the name of the new SSO server. If editing a server, this field is display only; it displays the name of the selected SSO server.
- **Authentication Type**—*Display only*. Displays the type of SSO server. The types currently supported by the security appliance are SiteMinder and SAML Browser Post Profile.
- **URL**—Enter the SSO server URL to which the security appliance makes SSO authentication requests.
- **Secret Key**—Enter a secret key used to encrypt authentication requests to the SSO server. Key characters can be any regular or shifted alphanumeric characters. There is no minimum or maximum number of characters. The secret key is similar to a password: you create it, save it, and configure it. It is configured on the security appliance, the SSO server, and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.
- **Maximum Retries**—Enter the number of times the security appliance retries a failed SSO authentication attempt before the authentication times-out. The range is from 1 to 5 retries inclusive, and the default is 3 retries.
- **Request Timeout**—Enter the number of seconds before a failed SSO authentication attempt times out. The range is from 1 to 30 seconds inclusive, and the default is 5 seconds.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Clientless SSL VPN Access

The Clientless SSL VPN Access panel lets you accomplish the following tasks:

- Enable or disable security appliance interfaces for Clientless SSL VPN sessions.
- Choose a port for Clientless SSL VPN connections.
- Set a global timeout value for Clientless SSL VPN sessions.
- Set a maximum number of simultaneous Clientless SSL VPN sessions.
- Configure the amount of security appliance memory that Clientless SSL VPN can use.

To configure Clientless SSL VPN services for individual users, the best practice is to use the **Configuration > VPN > General > Group Policy > Add/Edit > WebVPN** panel. Then use the **Configuration > Properties > Device Administration > User Accounts > VPN Policy** panel to assign the group policy to a user.

Fields

- **Configure access parameters for WebVPN**—Lets you enable or disable Clientless SSL VPN connections on configured security appliance interfaces.
 - **Interface**—Displays names of all configured interfaces.

- WebVPN Enabled—Displays current status for Clientless SSL VPN on the interface.
A green check next to Yes indicates that Clientless SSL VPN is enabled.
A red circle next to No indicates that Clientless SSL VPN is disabled.
- Enable/Disable—Click to enable or disable Clientless SSL VPN on the highlighted interface.
- Port Number—Enter the port number that you want to use for Clientless SSL VPN sessions. The default port is 443, for HTTPS traffic; the range is 1 through 65535. If you change the port number, All current Clientless SSL VPN connections terminate, and current users must reconnect. You also lose connectivity to ASDM, and a prompt displays, inviting you to reconnect.
- Default Idle Timeout—Enter the amount of time, in seconds, that a Clientless SSL VPN session can be idle before the security appliance terminates it. This value applies only if the Idle Timeout value in the group policy for the user is set to zero (0), which means there is no timeout value; otherwise the group policy Idle Timeout value takes precedence over the timeout you configure here. The minimum value you can enter is 1 minute. The default is 30 minutes (1800 seconds). Maximum is 24 hours (86400 seconds).

We recommend that you set this attribute to a short time period. This is because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the Simultaneous Logins attribute for the group policy is set to one, the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.

- Max. Sessions Limit—Enter the maximum number of Clientless SSL VPN sessions you want to allow. Be aware that the different ASA models support Clientless SSL VPN sessions as follows: ASA 5510 supports a maximum of 250; ASA 5520 maximum is 750; ASA 5540 maximum is 2500; ASA 5550 maximum is 5000.
- WebVPN Memory Size—Enter the percent of total memory or the amount of memory in kilobytes that you want to allocate to Clientless SSL VPN processes. The default is 50% of memory. Be aware that the different ASA models have different total amounts of memory as follows: ASA 5510—256 MB; ASA5520 —512 MB; ASA 5540—1GB, ASA 5550—4G. When you change the memory size, the new setting takes effect only after the system reboots.
- WebVPN Memory (unlabeled)—Choose to allocate memory for Clientless SSL VPN either as a percentage of total memory or as an amount of memory in kilobytes.
- Enable Tunnel Group Drop-down List on WebVPN Login— Check to include a drop-down list of configured tunnel groups on the Clientless SSL VPN end-user interface. Users select a tunnel group from this list when they log on. This field is checked by default. If you uncheck it, the user cannot select a tunnel group at logon.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

For More Information

[Clientless SSL VPN End User Set-up](#)

Configuring Smart Tunnel Access

The Smart Tunnels table displays the smart tunnel lists, each of which identifies one or more applications eligible for smart tunnel access, and its associated OS. Because each group policy or local user policy supports one smart tunnel list, you must group the nonbrowser-based applications to be supported into a smart tunnel list. Following the configuration of a list, you can assign it to one or more group policies or local user policies.

The **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels** window lets you do the following:

- To add a smart tunnel list and add applications to the list, choose **Add**. The Add Smart Tunnel List dialog box opens. After you name the list, click **Add** again. ASDM opens the Add Smart Tunnel Entry dialog box, which lets you assign the attributes of a smart tunnel to the list. After doing so and clicking OK, ASDM displays those attributes in the list. Repeat as needed to complete the list, then click **OK** in the Add Smart Tunnel List dialog box.
- To change a smart tunnel list, double-click the list or select the list in the table and click **Edit**. Then click **Add** to insert a new set of smart tunnel attributes into the list, or select an entry in the list and click **Edit** or **Delete**.
- To remove a list, select the list in the table and click **Delete**.

Following the configuration and assignment of a smart tunnel list, you can make a smart tunnel easy to use by adding a bookmark for the service and clicking the Enable Smart Tunnel Option in the Add or Edit Bookmark window.

The following sections describe smart tunnels and how to configure them to support nonbrowser-based applications:

- [About Smart Tunnels](#)
- [Why Smart Tunnels?](#)
- [Smart Tunnel Requirements, Restrictions, and Limitations](#)
- [Configuring a Smart Tunnel \(Lotus example\)](#)
- [Add or Edit Smart Tunnel List](#)
- [Add or Edit Smart Tunnel Entry](#)
- [Add or Edit Smart Tunnel Auto Sign-on Server List](#)
- [Add or Edit Smart Tunnel Auto Sign-on Server Entry](#)

About Smart Tunnels

A smart tunnel is a connection between a Winsock 2, TCP-based application and a private site, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server. You can identify applications to which you want to grant smart tunnel access, and specify the local path to each application. For applications running on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access.

Lotus SameTime, Microsoft Outlook, and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.

Configuring smart tunnels requires one of the following procedures, depending on whether the application is a client or is a web-enabled application:

- Create one or more smart tunnel lists of the client applications, then assign the list to the group policies or local user policies for whom you want to provide smart tunnel access.

- Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the DAPs, group policies, or local user policies for whom you want to provide smart tunnel access.

You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over clientless SSL VPN sessions.

Why Smart Tunnels?

Providing smart tunnel access is useful in the following cases:

- You are enabling clientless SSL VPN (the smart tunnel conduit).
- A plug-in is unavailable for the TCP-based application for which you want to enable access.
- You have chosen to configure port forwarding for a particular application.

Port forwarding requires that you know the ports the application uses. Remote users who do not have admin rights must connect the application to the local port on the local machine. Unlike full-tunnel clients, smart tunnel access does not require administrator privileges. Because of the flexibility of user rights for smart tunnels, port forwarding is primarily for legacy configurations.

Smart Tunnel Requirements, Restrictions, and Limitations

Smart tunnels have the following requirements:

- The remote host originating the smart tunnel connection must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
- Users of Microsoft Windows Vista who use smart tunnels or port forwarding must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.
- The browser must be enabled with Java, Microsoft ActiveX, or both.
- Smart tunnel support for Mac OS requires Safari 3.1.1 or later.

On Microsoft Windows, only Winsock 2, TCP-based applications are eligible for smart tunnel access.

On Mac OS, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel. The following types of applications do not work over a smart tunnel:

- Applications using dlopen or dlsym to locate libsocket calls
- Statically linked applications to locate libsocket calls
- Mac OS applications that use two-level name spaces.
- Mac OS, console-based applications, such as Telnet, SSH, and cURL.
- Mac OS, PowerPC-type applications. To determine the type of a Mac OS application, right-click its icon and select Get Info.

On Mac OS, only applications started from the portal page can establish smart tunnel sessions. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named `cisco_st`. If this user profile is not present, the session prompts the user to create one.

The following limitations apply to smart tunnels:

- If the remote computer requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. In this configuration, smart tunnels support only basic authentication.
- The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. Neither port forwarding nor the smart tunnel supports MAPI. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.
- The smart tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library on a Microsoft Windows OS. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.
- A group policy or local user policy supports no more than one list of applications eligible for smart tunnel access and one list of smart tunnel auto sign-on servers.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

Configuring a Smart Tunnel (Lotus example)

Configure a Smart Tunnel as follows:



Note

These example instructions provide the minimum instructions required to add smart tunnel support for an application. See the field descriptions in the sections that follow for more information.

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**.
- Step 2** Double-click the smart tunnel list to which you want to add an application; or click **Add** to create a list of applications, enter a name for this list in the List Name field, and click **Add**.
For example, click **Add** in the Smart Tunnels window, enter Lotus in the List Name field, and click **Add**.
- Step 3** Click **Add** in the Add or Edit Smart Tunnel List window.
- Step 4** Enter a string in the Application ID field to serve as a unique index to the entry within the smart tunnel list.
- Step 5** Enter the filename and extension of the application into the Process Name box.

[Table 38-1](#) shows example Application ID strings and the associated paths required to support Lotus.

Table 38-1 Smart Tunnel Example: Lotus 6.0 Thick Client with Domino Server 6.5.5

Application ID Example	Minimum Required Process Name
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

- Step 6** Select **Windows** next to OS.
- Step 7** Click **OK**.
- Step 8** Repeat Steps 3–7 for each application to add to the list.
- Step 9** Click **OK** in the Add or Edit Smart Tunnel List window.

- Step 10** Assign the list to the group policies and local user policies to which you want to provide smart tunnel access to the associated applications, as follows:
- To assign the list to a group policy, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and select the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
 - To assign the list to a local user policy, choose **Configuration > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and select the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

Add or Edit Smart Tunnel List

The Add Smart Tunnel List dialog box lets you add a list of smart tunnel entries to the security appliance configuration. The Edit Smart Tunnel List dialog box lets you modify the contents of the list.

Field

- List Name**—Enter a unique name for the list of applications or programs. The string can be up to 64 characters. Do not use spaces.

Following the configuration of the smart tunnel list, the list name appears next to the Smart Tunnel List attribute in the Clientless SSL VPN group policies and local user policies. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add or Edit Smart Tunnel Entry

The Add or Edit Smart Tunnel Entry dialog box lets you specify the attributes of an application in a smart tunnel list.

- Application ID**—Enter a string to name the entry in the smart tunnel list. The string is unique for the OS. It typically names the application to be granted smart tunnel access. To support multiple versions of an application for which you choose to specify different paths or hash values, you can use this attribute to differentiate entries, specifying the OS, and name and version of the application supported by each list entry. The string can be up to 64 characters.
- Process Name**—Enter the filename or path to the application. The string can be up to 128 characters. Mac OS requires the full path. Windows requires an exact match of this value to the right side of the application path on the remote host to qualify the application for smart tunnel access. If you specify only the filename for Windows, SSL VPN does not enforce a location restriction on the remote host to qualify the application for smart tunnel access.

If you specify a path and the user installed the application in another location, that application does not qualify. The application can reside on any path as long as the right side of the string matches the value you enter.

To authorize an application for smart tunnel access if it is present on one of several paths on the remote host, either specify only the name and extension of the application in this field; or create a unique smart tunnel entry for each path.



Note A sudden problem with smart tunnel access may be an indication that a *Process Name* value is not up-to-date with an application upgrade. For example, the default path to an application sometimes changes following the acquisition of the company that produces the application and the next application upgrade.

For Windows, if you want to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.

- OS—Select **Windows** or **Mac** to specify the host OS of the application.
- Hash—(Optional and applicable only for Windows) To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at <http://support.microsoft.com/kb/841290/>. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1 application** at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash.

The SHA-1 hash is always 40 hexadecimal characters.

Before authorizing an application for smart tunnel access, Clientless SSL VPN calculates the hash of the application matching the *Application ID*. It qualifies the application for smart tunnel access if the result matches the value of *Hash*.

Entering a hash provides a reasonable assurance that SSL VPN does not qualify an illegitimate file that matches the string you specified in the *Application ID*. Because the checksum varies with each version or patch of an application, the *Hash* you enter can only match one version or patch on the remote host. To specify a hash for more than one version of an application, create a unique smart tunnel entry for each *Hash* value.



Note You must update the smart tunnel list in the future if you enter *Hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *Hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a hash.

Following the configuration of the smart tunnel list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** and select the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
- To assign the list to a local user policy, choose **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** and select the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add or Edit Smart Tunnel Auto Sign-on Server List

The Add Smart Tunnel Auto Sign-on Server List dialog box lets you add one or more lists of servers for which to automate the submission of login credentials during smart tunnel setup. The Edit Smart Tunnel Auto-signon Server List dialog box lets you modify the contents of these lists.

Field

- **List Name**—Enter a unique name for the list of remote servers. The string can be up to 64 characters. Do not use spaces.

Following the configuration of the smart tunnel auto sign-on list, the list name appears next to the Auto Sign-on Server List attribute under Smart Tunnel in the Clientless SSL VPN group policy and local user policy configurations. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add or Edit Smart Tunnel Auto Sign-on Server Entry

The Add or Edit Smart Tunnel Entry dialog box lets you identify a server to be added to a smart tunnel auto sign-on list. You can identify it by its host name, or IP address and subnet mask.



Caution

Use the address format used in the source code of the web pages on the intranet. If you are configuring smart tunnel auto sign-on for browser access and some web pages use host names and others use IP addresses, or you do not know, specify both in different smart tunnel auto sign-on entries. Otherwise, if a link on a web page uses a different format than the one you specify, it will fail when the user clicks it.

- **Host name**—Enter a host name or wildcard mask to auto-authenticate to. For example, enter *.example.com. Using this option protects the configuration from dynamic changes to IP addresses.
- **IP Address**—Enter an IP address to auto-authenticate to.
- **Subnet Mask**—Sub-network of hosts associated with the IP address.
- **Use Windows domain name with user name (Optional)** —Check to add the Windows domain to the username if authentication requires it. If you do so, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies or local user policies.

Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal**, find the Smart Tunnel area, and select the list name from the drop-down list next to the Auto Sign-on Server List attribute.
- To assign the list to a local user policy, choose **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**, find the Smart Tunnel area, and select the list name from the drop-down list next to the Auto Sign-on Server List attribute.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Customization Objects

You can customize all end-user visible content on the clientless SSL VPN portal. To do so, you create an XML customization object, using an XML template, the Customization Editor in ASDM, or by exporting and editing an already existing customization object, which you then reimport to the security appliance.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.



Note

Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file *before* you upgrade to Version 8.0.

From the current pane, you can add a new customization object, based on a template, or you can modify an already-imported customization object.

Fields

Add—Click to invoke the Add Customization pane, which lets you make a copy of the default customization object and save it with a unique name. Then you can use the ASDM SSL VPN Customization Editor to modify it to suit your requirements.

Edit—Click to edit an existing, highlighted customization object. Doing so invokes the SSL VPN Customization Editor.

Delete—Click to delete a customization object.

Import—Click to import a customization object, which is an XML file. For information about creating such an XML file, click this link: [Creating XML-Based Portal Customization Objects and URL Lists](#).

Export—Click to export an exiting, highlighted customization object. Doing so lets you edit the object, and then reimport it to this security appliance or to another one.

Customization Objects—Lists the existing customization objects on the security appliance.

OnScreen Keyboard—Specify when to display the OnScreen Keyboard to end users. This keyboard provides additional security by eliminating the need to enter keystrokes on a physical keyboard for passwords when users log on or otherwise authenticate.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add Customization Object

To add a customization object, create a copy of and provide a unique name for the DfltCustomization object. Then you can modify or edit it to meet your requirements.

Field

Customization Object Name—Enter a name for the new customization object. Maximum 64 characters, no spaces.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Import/Export Customization Object

You can import or export already-existing customization objects. Import an object that you want to apply to end users. Export a customization object already resident on the security appliance for editing purposes, after which you can reimport it.

Fields

- **Customization Object Name**—Identify the customization object by name. Maximum 64 characters, no spaces.
- **Select a file**—Choose the method by which you want to import or export the customization file.
 - **Local computer**—Choose this method to import a file that resides on the local PC.
 - **Path**—Provide the path to the file.

- Browse Local Files—Browse to the path for the file.
- Flash file system—Choose this method to export a file that resides on the security appliance.
- Path—Provide the path to the file.
- Browse Flash—Browse to the path for the file.
- Remote server—Select this option to import a customization file that resides on a remote server accessible from the security appliance.
- Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
- Import/Export Now—Click to import or export the file.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Creating XML-Based Portal Customization Objects and URL Lists

This section includes the following topics:

- [Understanding the XML Customization File Structure](#)
- [Customization Example](#)
- [Using the Customization Template](#)

Understanding the XML Customization File Structure

Table 38-2 presents the file structure for an XML customization object.



Note

An empty tag `<param></param>` in an XML customization file is the equivalent of a CLI command with a trivial value:

```
(hostname)# param value ""
```

Absence of a parameter/tag results in a default/inherited value, while presence results in setting the parameter/tag value even it is an empty string.

Table 38-2 XML-Based Customization File Structure

Tag	Type	Values	Preset value	Description
custom	node			Root tag
auth-page	node			Tag-container of authentication page configuration

Table 38-2 XML-Based Customization File Structure

window	node			Browser window
title-text	string	Arbitrary string	empty string	
title-panel	node			The page top panel with a logo and a text
mode	text	enable disable	disable	
text	text	Arbitrary string	empty string	
logo-url	text	Arbitrary URL	empty image URL	
copyright-panel	node			The page bottom panel with a copyright information
mode	text	enable disable	disable	
text	text	Arbitrary URL	empty string	
info-panel	node			The panel with a custom text and image
mode	string	enable disable	disable	
image-position	string	above below	above	The image position, relative to text
image-url	string	Arbitrary URL	empty image	
text	string	Arbitrary string	empty string	
logon-form	node			The form with username, password, group prompt
title-text	string	Arbitrary string	Logon	
message-text	string	Arbitrary string	empty string	
username-prompt-text	string	Arbitrary string	Username	
password-prompt-text	string	Arbitrary string	Password	
internal-password-prompt-text	string	Arbitrary string	Internal Password	
group-prompt-text	string	Arbitrary string	Group	
submit-button-text	string	Arbitrary string	Logon	
logout-form	node			The form with a logout message and the buttons to login or close the window
title-text	string	Arbitrary string	Logout	
message-text	string	Arbitrary string	Empty string	
login-button-text	string	Arbitrary string	Login	

Table 38-2 XML-Based Customization File Structure

close-button-text	string	Arbitrary string	Close window	
language-selector	node			The drop-down box to select a language
mode	string	enable disable	disable	
title	text		Language	The prompt text to select language
language	node (multiple)			
code	string			
text	string			
portal	node			Tag-container of the portal page configuration
window	node			see authentication page description
title-text	string	Arbitrary string	Empty string	
title-panel	node			see authentication page description
mode	string	enable disable	Disable	
text	string	Arbitrary string	Empty string	
logo-url	string	Arbitrary URL	Empty image URL	
navigation-panel	node			The panel on the left with application tabs
mode	string	enable disable	enable	
application	node (multiple)		N/A	The node changes defaults for the configured (by id) application
id	string	For stock application web-access file-access app-access net-access help For ins: Unique plug-in	N/A	
tab-title	string		N/A	

Table 38-2 XML-Based Customization File Structure

order	number		N/A	Value used to sort elements. The default element order values have step 1000, 2000, 3000, etc. For example, to insert an element between the first and second element, use a value 1001 – 1999.
url-list-title	string		N/A	If the application has bookmarks, the title for the pane with grouped bookmarks
mode	string	enable disable	N/A	
toolbar	node			
mode	string	enable disable	Enable	
prompt-box-title	string	Arbitrary string	Address	Title for URL prompt box
browse-button-text	string	Arbitrary string	Browse	Browse button text
logout-prompt-text	string	Arbitrary string	Logout	
column	node (multiple)			One column will be shown by default
width	string		N/A	
order	number		N/A	Value used to sort elements.
url-lists	node			URL lists are considered to be default elements on the portal home page, if they are not explicitly disabled
mode	string	group nogroup	group	Modes: group – elements grouped by application type i.e. Web Bookmarks, File Bookmarks) no-group – url-lists are shown in separate panes disable – do not show URL lists by default
pane	node (multiple)			Allows to configure extra panes

Table 38-2 XML-Based Customization File Structure

mode	string	enable/disable		Used to temporarily disable the pane without removing its configuration
title	string			
type	string			Supported types: RSS IMAGE TEXT HTML
url	string			URL for RSS, IMAGE or HTML type panes
url-mode	string			Modes: mangle, no-mangle
text	string			Text for TEXT type panes
column	number			

Customization Example

The following example illustrates the following customization options:

- Hides tab for the File access application
- Changes title and order of Web Access application
- Defines two columns on the home page
- Adds an RSS pane
- Adds three panes (text, image, and html) at the top of second pane

```
<custom name="Default">
  <auth-page>

    <window>
      <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
      <mode>enable</mode>
      <text l10n="yes">XYZ WebVPN</text>
      <logo-url>http://www.xyz.com/images/XYZ.gif</logo-url>
    </title-panel>

    <copyright>
      <mode>enable</mode>
      <text l10n="yes">(c)Copyright, XYZ Inc., 2006</text>
    </copyright>

    <info-panel>
```

```

        <mode>enable</mode>
        <image-url>/+CSCOE+/custom/XYZ.jpg</image-url>
    <text l10n="yes">
        <![CDATA[
            <div>
                <b>Welcome to WebVPN !.</b>
            </div>
        ]]>
    </text>
</info-panel>

<logon-form>
    <form>
        <title-text l10n="yes">title WebVPN Logon</title>
        <message-text l10n="yes">message WebVPN Logon</title>
        <username-prompt-text l10n="yes">Username</username-prompt-text>
        <password-prompt-text l10n="yes">Password</password-prompt-text>
        <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
        <group-prompt-text l10n="yes">Group</group-prompt-text>
        <submit-button-text l10n="yes">Logon</submit-button-text>
    </form>
</logon-form>

<logout-form>
    <form>
        <title-text l10n="yes">title WebVPN Logon</title>
        <message-text l10n="yes">message WebVPN Logon</title>
        <login-button-text l10n="yes">Login</login-button-text>
        <close-button-text l10n="yes">Logon</close-button-text>
    </form>
</logout-form>

<language-selector>
    <language>
        <code l10n="yes">code1</code>
        <text l10n="yes">text1</text>
    </language>
    <language>
        <code l10n="yes">code2</code>
        <text l10n="yes">text2</text>
    </language>
</language-selector>

</auth-page>

<portal>

    <window>
        <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
        <mode>enable</mode>
        <text l10n="yes">XYZ WebVPN</text>
        <logo-url>http://www.xyz.com/logo.gif</logo-url>
    </title-panel>

    <navigation-panel>
        <mode>enable</mode>
    </navigation-panel>

    <application>
        <id>file-access</id>

```



```

        <mode>disable</mode>
    </application>
    <application>
        <id>web-access</id>
        <tab-title>XYZ Intranet</tab-title>
        <order>3001</order>
    </application>

    <column>
        <order>2</order>
        <width>40%</width>
    </column>
    <column>
        <order>1</order>
        <width>60%</width>
    </column>

    <url-lists>
        <mode>no-group</mode>
    </url-lists>

    <pane>
        <id>rss_pane</id>
        <type>RSS</type>
        <url>rss.xyz.com?id=78</url>
    </pane>

    <pane>
        <id>text_pane</id>
        <type>TEXT</type>
        <url>rss.xyz.com?id=78</url>
        <column>1</column>
        <row>0</row>
        <text>Welcome to XYZ WebVPN Service</text>
    </pane>

    <pane>
        <type>IMAGE</type>
        <url>http://www.xyz.com/logo.gif</url>
        <column>1</column>
        <row>2</row>
    </pane>

    <pane>
        <type>HTML</type>
        <title>XYZ news</title>
        <url>http://www.xyz.com/news.html</url>
        <column>1</column>
        <row>3</row>
    </pane>

</portal>

</custom>

```

Using the Customization Template

A customization template, named *Template*, contains all currently employed tags with corresponding comments that describe how to use them. Use the export command to download the customization template from the security appliance, as follows:

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

You cannot change or delete the file *Template*. When you export it as in this example, you are saving it to a new name, *default.xml*. After you make your changes to this file, using it to create a customization object that meets the needs of your organization, you import it to the security appliance, either as *default.xml* or another name of your choosing. For example,

```
hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#
```

where you import an XML object called *custom.xml* and name it *General* on the security appliance.

The Customization Template

The customization template, named *Template*, follows.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
```

```
Copyright (c) 2007,2008 by Cisco Systems, Inc.
All rights reserved.
```

Note: all whitespaces in tag values are significant and preserved.

```
Tag: custom
Description: Root customization tag
```

```
Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes. Each language code is
       a set dash-separated alphanumeric characters, started with
       alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us
```

```
Tag: custom/default-language
Description: Language code that is selected when the client and the server
           were not able to negotiate the language automatically.
           For example the set of languages configured in the browser
           is "en,ja", and the list of languages, specified by
           'custom/languages' tag is "cn,fr", the default-language will be
           used.
Value: string, containing one of the language coded, specified in
       'custom/languages' tag above.
Default value: en-us
```

```
*****
```

```
Tag: custom/auth-page
Description: Contains authentication page settings
```

```
*****
```

```
Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window
```

```
Tag: custom/auth-page/window/title-text
Description: The title of the browser window of the authentication page
Value: arbitrary string
Default value: Browser's default value
```

```
*****
```

Tag: custom/auth-page/title-panel
Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder, lighter etc.
Default value: empty string

Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string

Tag: custom/auth-page/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value: no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string

Default value: empty string

Tag: custom/auth-page/info-panel

Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode

Description: The information panel mode

Value: enable|disable

Default value: disable

Tag: custom/auth-page/info-panel/image-position

Description: Position of the image, above or below the informational panel text

Values: above|below

Default value: above

Tag: custom/auth-page/info-panel/image-url

Description: URL of the information panel image (imported via "import webvpn webcontent")

Value: URL string

Default value: empty image URL

Tag: custom/auth-page/info-panel/text

Description: Text of the information panel

Text: arbitrary string

Default value: empty string

Tag: custom/auth-page/logon-form

Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text

Description: The logon form title text

Value: arbitrary string

Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text

Description: The message inside of the logon form

Value: arbitrary string

Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text

Description: The username prompt text

Value: arbitrary string

Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text

Description: The password prompt text

Value: arbitrary string

Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text

Description: The internal password prompt text

Value: arbitrary string

Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text

Description: The group selector prompt text

Value: arbitrary string

Default value: "Group"

Tag: custom/auth-page/logon-form/submit-button-text

Description: The submit button text
 Value: arbitrary string
 Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first
 Description: Sets internal password first in the order
 Value: yes|no
 Default value: no

Tag: custom/auth-page/logon-form/title-font-color
 Description: The font color of the logon form title
 Value: HTML color format, for example #FFFFFF
 Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color
 Description: The background color of the logon form title
 Value: HTML color format, for example #FFFFFF
 Default value: #000000

Tag: custom/auth-page/logon-form/font-color
 Description: The font color of the logon form
 Value: HTML color format, for example #FFFFFF
 Default value: #000000

Tag: custom/auth-page/logon-form/background-color
 Description: The background color of the logon form
 Value: HTML color format, for example #FFFFFF
 Default value: #000000

Tag: custom/auth-page/logout-form
 Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text
 Description: The logout form title text
 Value: arbitrary string
 Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text
 Description: The logout form message text
 Value: arbitrary string
 Default value: Goodbye.

For your own security, please:
 Clear the browser's cache
 Delete any downloaded files
 Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text
 Description: The text of the button sending the user to the logon page
 Value: arbitrary string
 Default value: "Logon"

Tag: custom/auth-page/language-selector
 Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode
 Description: The language selector mode
 Value: enable|disable

Default value: disable

Tag: custom/auth-page/language-selector/title

Description: The language selector title

Value: arbitrary string

Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)

Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code

Description: The code of the language

Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text

Description: The text of the language in the language selector drop-down box

Value (required): arbitrary string

Tag: custom/portal

Description: Contains portal page settings

Tag: custom/portal/window

Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text

Description: The title of the browser window of the portal page

Value: arbitrary string

Default value: Browser's default value

Tag: custom/portal/title-panel

Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode

Description: The title panel mode

Value: enable|disable

Default value: disable

Tag: custom/portal/title-panel/text

Description: The title panel text.

Value: arbitrary string

Default value: empty string

Tag: custom/portal/title-panel/logo-url

Description: The URL of the logo image (imported via "import webvpn webcontent")

Value: URL string

Default value: empty image URL

Tag: custom/portal/title-panel/background-color

Description: The background color of the title panel

Value: HTML color format, for example #FFFFFF

Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color

Description: The background color of the title panel

Value: HTML color format, for example #FFFFFF

Default value: #000000

Tag: custom/portal/title-panel/font-weight

Description: The font weight
 Value: CSS font size value, for example bold, bolder, lighter etc.
 Default value: empty string

Tag: custom/portal/title-panel/font-size
 Description: The font size
 Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
 Default value: empty string

Tag: custom/portal/title-panel/gradient
 Description: Specifies using the background color gradient
 Value: yes|no
 Default value: no

Tag: custom/portal/title-panel/style
 Description: CSS style for title text
 Value: CSS style string
 Default value: empty string

Tag: custom/portal/application (multiple)
 Description: Contains the application setting

Tag: custom/portal/application/mode
 Description: The application mode
 Value: enable|disable
 Default value: enable

Tag: custom/portal/application/id
 Description: The application ID. Standard application ID's are: home, web-access, file-access, app-access, network-access, help
 Value: The application ID string
 Default value: empty string

Tag: custom/portal/application/tab-title
 Description: The application tab text in the navigation panel
 Value: arbitrary string
 Default value: empty string

Tag: custom/portal/application/order
 Description: The order of the application's tab in the navigation panel. Applications with lesser order go first.
 Value: arbitrary number
 Default value: 1000

Tag: custom/portal/application/url-list-title
 Description: The title of the application's URL list pane (in group mode)
 Value: arbitrary string
 Default value: Tab title value concatenated with "Bookmarks"

Tag: custom/portal/navigation-panel
 Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode
 Description: The navigation panel mode
 Value: enable|disable
 Default value: enable

Tag: custom/portal/toolbar

Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode

Description: The toolbar mode

Value: enable|disable

Default value: enable

Tag: custom/portal/toolbar/prompt-box-title

Description: The universal prompt box title

Value: arbitrary string

Default value: "Address"

Tag: custom/portal/toolbar/browse-button-text

Description: The browse button text

Value: arbitrary string

Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text

Description: The logout prompt text

Value: arbitrary string

Default value: "Logout"

Tag: custom/portal/column (multiple)

Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order

Description: The order the column from left to right. Columns with lesser order values go first

Value: arbitrary number

Default value: 0

Tag: custom/portal/column/width

Description: The home page column width

Value: percent

Default value: default value set by browser

Note: The actual width may be increased by browser to accommodate content

Tag: custom/portal/url-lists

Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode

Description: Specifies how to display URL lists on the home page:

group URL lists by application (group) or

show individual URL lists (nogroup).

URL lists fill out cells of the configured columns, which are not taken by custom panes.

Use the attribute value "nodisplay" to not show URL lists on the home page.

Value: group|nogroup|nodisplay

Default value: group

Tag: custom/portal/pane (multiple)

Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode

Description: The mode of the pane

Value: enable|disable


```

Default value: disable

Tag: custom/portal/pane/title
Description: The title of the pane
Value: arbitrary string
Default value: empty string

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane. Supported types:
    TEXT - inline arbitrary text, may contain HTML tags;
    HTML - HTML content specified by URL shown in the individual iframe;
    IMAGE - image specified by URL
    RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type  HTML,IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser

*****

Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network

Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
Default value: Start AnyConnect

-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>

```

```

<default-language>en</default-language>
</localization>
= <auth-page>
= <window>
= <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
= <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
= <language>
<code>en</code>
<text>English</text>
</language>
= <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
= <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
= <language>
<code>ru</code>
<text>?????? (Russian)</text>
</language>
= <language>
<code>ua</code>
<text>???????? (Ukrainian)</text>
</language>
</language-selector>
= <logon-form>
= <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
= <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
= <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
= <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.
]]>
</message-text>
= <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
= <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>

```

```

</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>

```

```

- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
= <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
= <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
= <portal>
= <title-panel>
<mode>enable</mode>
= <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/cisco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
= <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
= <font-size>
- <![CDATA[
larger
]]>
</font-size>
= <font-color>
- <![CDATA[
#800000
]]>
</font-color>
= <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
= <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
= <application>
<mode>enable</mode>
<id>web-access</id>
= <tab-title l10n="yes">
- <![CDATA[
Web Applications
]]>
</tab-title>

```

```

- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>

```

```

<pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
<pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
<pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
<url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>

```

Help Customization

The security appliance displays help content on the application panels during clientless sessions. Each clientless application panel displays its own help file content using a predetermined filename. For example, the help content displayed on the Application Access panel is from the file named app-access-hlp.inc. [Table 38-3](#) shows the clientless application panels and predetermined filenames for the help content.

Table 38-3 Clientless Applications

Application Type	Panel	Filename
Standard	Application Access	app-access-hlp.inc
Standard	Browse Networks	file-access-hlp.inc
Standard	AnyConnect Client	net-access-hlp.inc
Standard	Web Access	web-access-hlp.inc
Plug-in	MetaFrame Access	ica-hlp.inc
Plug-in	Terminal Servers	rdp-hlp.inc

Table 38-3 **Clientless Applications**

Application Type	Panel	Filename
Plug-in	Telnet/SSH Servers	ssh,telnet-hlp.inc
Plug-in	VNC Connections	vnc-hlp.inc

You can customize the help files provided by Cisco or create help files in other languages. Then use the Import button to copy them to the flash memory of the security appliance for display during subsequent clientless sessions. You can also export previously imported help content files, customize them, and reimport them to flash memory.

The following sections describe how to customize or create help content visible on clientless sessions:

- [Customizing a Help File Provided by Cisco](#)
- [Creating Help Files for Languages Not Provided by Cisco](#)

Fields

Import—Click to launch the Import Application Help Content dialog, where you can import new help content to flash memory for display during clientless sessions.

Export—Click to retrieve previously imported help content selected from the table.

Delete—Click to delete previously imported help content selected from the table.

Language—Displays the abbreviation of the language rendered by the browser. This field is *not* used for file translation; it indicates the language used in the file. To identify the name of a language associated with an abbreviation in the table, display the list of languages rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:

- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
- Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.

Filename—Displays the filename the help content file was imported as.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Customizing a Help File Provided by Cisco

To customize a help file provided by Cisco, you need to get a copy of the file from the flash memory card first. Get the copy and customize it as follows:

-
- Step 1** Use your browser to establish a clientless session with the security appliance.

- Step 2** Display the help file by appending the string in “URL of Help File in Flash Memory of the Security Appliance” in [Table 38-4](#), to the address of the security appliance, substituting *language* as described below, then press Enter.

Table 38-4 Help Files Provided by Cisco for Clientless Applications

Application Type	Panel	URL of Help File in Flash Memory of the Security Appliance
Standard	Application Access	/+CSCOE+/help/ <i>language</i> /app-access-hlp.inc
Standard	Browse Networks	/+CSCOE+/help/ <i>language</i> /file-access-hlp.inc
Standard	AnyConnect Client	/+CSCOE+/help/ <i>language</i> /net-access-hlp.inc
Standard	Web Access	/+CSCOE+/help/ <i>language</i> /web-access-hlp.inc
Plug-in	Terminal Servers	/+CSCOE+/help/ <i>language</i> /rdp-hlp.inc
Plug-in	Telnet/SSH Servers	/+CSCOE+/help/ <i>language</i> /ssh,telnet-hlp.inc
Plug-in	VNC Connections	/+CSCOE+/help/ <i>language</i> /vnc-hlp.inc

language is the abbreviation for the language rendered by the browser. It is *not* used for file translation; it indicates the language used in the file. For help files provided by Cisco in English, enter the abbreviation **en**.

The following example address displays the English version of the Terminal Servers help:

https://address_of_security_appliance/+CSCOE+/help/en/rdp-hlp.inc

- Step 3** Choose File > Save (Page) As.



Caution

Do not change the contents of the File name box.

- Step 4** Change the Save as type option to “Web Page, HTML only” and click Save.

- Step 5** Use your preferred HTML editor to customize the file.



Note

You can use most HTML tags, but do *not* use tags that define the document and its structure (e.g., do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the tag, and the <p>, , , and tags to structure content.

- Step 6** Save the file as HTML only, using the original filename and extension.

- Step 7** Make sure the filename matches the one in [Table 38-4](#), and that it does not have an extra filename extension.

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the modified help file into flash memory.

Creating Help Files for Languages Not Provided by Cisco

Use standard HTML to create help files in other languages. We recommend creating a separate folder for each language you want to support.

**Note**

You can use most HTML tags, but do *not* use tags that define the document and its structure (e.g., do not use <html>, <title>, <body>, <head>, <h1>, <h2>, etc. You can use character tags, such as the tag, and the <p>, , , and tags to structure content.

Save the file as HTML only. Use the filename in the Filename column of [Table 38-3](#).

Return to ASDM and choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization > Import** to import the new help file into flash memory.

Import/Export Application Help Content

Use the Import Application Help Content dialog box to import help files to flash memory for display on the portal pages during clientless sessions. Use the Export Application Help Content dialog box to retrieve previously imported help files for subsequent editing.

Fields

Language—For the Import Application Help Content dialog box only, this field specifies the language rendered by the browser. (This Language field is inactive in the Export Application Help Content dialog box.) This field is not used for file translation; it indicates the language used in the file. Click the dots next to the Language field, double-click the row containing the language used in the help file in the Browse Language Code dialog box, confirm the abbreviation in the Language Code field matches the abbreviation in the row, and click **OK**. If the language for which you want to provide help content is not present in the Browse Language Code dialog box, enter the abbreviation for the language you want into the Language Code field and click **OK**, or enter it into the Language text box to the left of the dots. To identify the abbreviation for the language of a help file to be imported if it is not present in the Browse Language Code dialog box, display the list of languages and abbreviations rendered by your browser. For example, a dialog window displays the languages and associated language codes when you use one of the following procedures:

- Open Internet Explorer and choose **Tools > Internet Options > Languages > Add**.
- Open Mozilla Firefox and choose **Tools > Options > Advanced > General**, click **Choose** next to Languages, and click **Select a language to add**.

File Name—If you are importing, specify the file name from the drop-down list for the new help content file. If you are exporting, this field is unavailable.

Select a File—Configure the parameters for the source file (if importing) or destination file (if exporting):

Local computer—Select if the source or destination file is on a local computer:

- **Path**—Identify the path of the source or destination file.
- **Browse Local Files**—Click to browse the local computer for the source or destination file.

Flash file system—Select if the source or destination file is located in flash memory on the security appliance:

- **Path**—Identify the path of the source or destination file in flash memory.
- **Browse Flash**—Click to browse the flash memory for the source or destination file.

Remote server—Select if the source or destination file is on a remote server:

- **Path**—Select the file transfer (copy) method, either ftp, tftp, or http (for importing only), and specify the path.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configuring Browser Access to Client-Server Plug-ins

The Client-Server Plug-in table displays the plug-ins the security appliance makes available to browsers in Clientless SSL VPN sessions.

To add, change, or remove a plug-in, do one of the following:

- To add a plug-in, click **Import**. The Import Plug-ins dialog box opens.
- To remove a plug-in, select it and click **Delete**.

The following sections describe the integration of browser plug-ins for Clientless SSL VPN browser access:

- [About Installing Browser Plug-ins](#)
- [Plug-in Requirements and Restrictions](#)
- [Preparing the Security Appliance for a Plug-in](#)
- [Installing Plug-ins Redistributed by Cisco](#)
- [Assembling and Installing Third-Party Plug-ins—Example: Citrix Java Presentation Server Client](#)
- [Assembling and Installing Third-Party Plug-ins—Example: TN 5250 Client Plug-in](#)
- [Assembling and Installing Third-Party Plug-ins—Example: TN 3270 Client Plug-in](#)

About Installing Browser Plug-ins

A browser plug-in is a separate program that a web browser invokes to perform a dedicated function, such as connect a client to a server within the browser window. The security appliance lets you import plug-ins for download to remote browsers in Clientless SSL VPN sessions. Of course, Cisco tests the plug-ins it redistributes, and in some cases, tests the connectivity of plug-ins we cannot redistribute. However, we do not recommend importing plug-ins that support streaming media at this time.



Note

Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

The security appliance does the following when you install a plug-in onto the flash device:

- (Cisco-distributed plug-ins only) Unpacks the jar file specified in the *URL*.
- Writes the file to the `cisco-config/97/plugin` directory on the security appliance file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future Clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page.

Table 38-5 shows the changes to the main menu and address field of the portal page when you add the plug-ins described in the following sections.

Table 38-5 *Effects of Plug-ins on the Clientless SSL VPN Portal Page*

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
tn3270	TN3270	tn3270://
tn5250	TN5250	tn5250://
vnc	VNC Client	vnc://



Note

A secondary security appliance obtains the plug-ins from the primary security appliance.

When the user in a Clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.



Note

Some Java plug-ins may report a status of connected or online even when a session to the destination service is not set up. The open-source plug-in reports the status, not the security appliance.

Before installing the first plug-in, you must follow the instructions in the next section.

Plug-in Requirements and Restrictions

Clientless SSL VPN must be enabled on the security appliance to provide remote access to the plug-ins.

The minimum access rights required for remote use belong to the guest privilege mode. The plug-ins automatically install or update the Java version required on the remote computer.

A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.

Preparing the Security Appliance for a Plug-in

Before installing a plug-in, prepare the security appliance as follows:

- Step 1** Make sure Clientless SSL VPN (“webvpn”) is enabled on a security appliance interface.
- Step 2** Install an SSL certificate onto the security appliance interface to which remote users use a fully-qualified domain name (FQDN) to connect.

**Note**

Do not specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN.

Go to the section that identifies the type of plug-in you want to provide for Clientless SSL VPN access.

- [Installing Plug-ins Redistributed by Cisco](#)
- [Assembling and Installing Third-Party Plug-ins—Example: Citrix Java Presentation Server Client](#)
- [Assembling and Installing Third-Party Plug-ins—Example: TN 5250 Client Plug-in](#)
- [Assembling and Installing Third-Party Plug-ins—Example: TN 3270 Client Plug-in](#)

Installing Plug-ins Redistributed by Cisco

Cisco redistributes the following, open-source, Java-based components to be accessed as plug-ins for web browsers in Clientless SSL VPN sessions:

- rdp-plugin.jar—The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is <http://properjavardp.sourceforge.net/>.
- ssh-plugin.jar—The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell or Telnet connection to a remote computer. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is <http://javassh.org/>.

**Note**

The ssh-plugin.jar provides support for both SSH and Telnet protocols. The SSH client supports SSH Version 1.0.

- vnc-plugin.jar—The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is <http://www.tightvnc.com>.

To retrieve a plug-in redistributed by Cisco and import it into the security appliance, perform the following steps:

- Step 1** Create a temporary directory named **plugins** on the computer you use to establish ASDM sessions with the security appliance.
- Step 2** Download the plug-ins you want from the Cisco website to the **plugins** directory.
- Step 3** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.

This window displays the plug-ins that are available to Clientless SSL sessions.
- Step 4** Click **Import**.

The Import Client-Server Plug-in dialog box opens.
- Step 5** Use the descriptions below to enter the field values.

Fields

The Import Client-Server Plug-in dialog box displays the following fields:

- Plug-in Name—Select one of the following values:
 - **ica** to provide plug-in access to Citrix MetaFrame services. Then specify the path to the ica-plugin.jar file in the Remote Server field, as described below.
 - **rdp** to provide plug-in access to Remote Desktop Protocol services. Then specify the path to the rdp-plugin.jar file in the Remote Server field.
 - **ssh,telnet** to provide plug-in access to *both* Secure Shell and Telnet services. Then specify the path to the ssh-plugin.jar file in the Remote Server field.
 - **tn3270**—to emulate a 3270 terminal to connect to an IBM mainframe.
 - **tn5250**—to emulate a 5250 terminal to connect to an IBM mainframe.
 - **vnc** to provide plug-in access to Virtual Network Computing services. Then specify the path to the vnc-plugin.jar file in the Remote Server field.



Note Any undocumented options in this menu are experimental and are not supported.

- Select a file—Click one of the following options and insert a path into its test box.
 - Local computer—Click to retrieve the plug-in from the computer with which you have established the ASDM session. Enter the location and name of the plug-in in the associated Path field, or click **Browse Local Files** and navigate to the plug-in, select it, then click **Select**.
 - Flash file system—Click if the plug-in is present on the file system of the security appliance. Enter the location and name of the plug-in in the associated Path field, or click **Browse Flash** and navigate to the plug-in, select it, then click **OK**.
 - Remote Server—Click to retrieve the plug-in from a host running an FTP or TFTP server. Select **ftp**, **tftp**, or **HTTP** in the drop-down menu next to the associated Path attribute, depending on which service is running on the remote server. Enter the host name or address of the server and the path to the plug-in in the adjacent text box.

Step 6 Click **Import Now**.

Click **Apply**.

The plug-in is now available for future Clientless SSL VPN sessions.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Assembling and Installing Third-Party Plug-ins—Example: Citrix Java Presentation Server Client

The open framework of the security appliance lets you add plug-ins to support third-party Java client/server applications. As an example of how to provide Clientless SSL VPN browser access to third-party plug-ins, this section describes how to add Clientless SSL VPN support for the Citrix Presentation Server Client.

**Caution**

Cisco does not provide direct support for or recommend any particular plug-ins that are not redistributed by Cisco. As a provider of Clientless SSL VPN services, you are responsible for reviewing and complying with any license agreements required for the use of plug-ins.

With a Citrix plug-in installed on the security appliance, Clientless SSL VPN users can use a connection to the security appliance to access Citrix MetaFrame services.

A stateful failover does not retain sessions established using the Citrix plug-in. Citrix users must reauthenticate after failover.

Follow the sequence of instructions in the following sections to provide access to the Citrix plug-in:

- [Preparing the Citrix MetaFrame Server for Clientless SSL VPN Access](#)
- [Creating and Installing the Citrix Plug-in](#)

Preparing the Citrix MetaFrame Server for Clientless SSL VPN Access

The security appliance performs the connectivity functions of the Citrix secure gateway when the Citrix client connects to the Citrix MetaFrame Server. Therefore, you must prepare the Citrix MetaFrame Server, as indicated in the following caution statement:

**Caution**

Configure the Citrix Web Interface software to operate in a mode that does not use the (Citrix) “secure gateway.” Otherwise, the Citrix client cannot connect to the Citrix MetaFrame Server.

**Note**

You must follow the instructions in the [“Preparing the Security Appliance for a Plug-in”](#) section on [page 38-65](#) before using the next section, if you are not already providing support for a plug-in.

Creating and Installing the Citrix Plug-in

Create and install the Citrix plug-in, as follows:

Step 1 Install a Java Development Kit (JDK) Version 1.5.0_8 on a Linux server.

**Note**

Follow each of the remaining steps except for the last on this Linux server.

Step 2 Create a directory to store the plug-in to be created later in these instructions. For example, **mkdir plugins**

Step 3 Create a subdirectory to store files specific to the plug-in to be built. For example, **mkdir plugins/ica**

Step 4 Download the Citrix Presentation Server Client file to the plugins/ica subdirectory.

**Note**

At the time of publication of this document, Citrix provided the Citrix Presentation Server Clients file for download on <http://www.citrix.com> at the following path: **Downloads > Clients**.

- Step 5** Unpack the following files from the Citrix Presentation Server Client file into the `plugins/ica` subdirectory:
- JICA-configN.jar
 - JICA-coreN.jar
- Step 6** Download the zip file containing the machine instructions needed to generate a Citrix plug-in for the security appliance, from the Cisco web site to the `plugins/ica` subdirectory, and extract the files.
- The following files extract from the zip file:
- desktop.html
 - icon.gif
 - lib.js
 - manifest.xml
- Cisco customized these files for use with the Citrix plug-in.
- After you build the Citrix plug-in and import it to the security appliance, and the remote browser downloads it, the portal page displays the icon.gif image. The user clicks the image to establish a connection with a Citrix server.
- The plug-in incorporates the image in the icon.gif file, so following the generation of the plug-in, you need to import only the plug-in to the security appliance.
- Step 7** Enter the following command from the `plugins/ica` subdirectory to create the Citrix plug-in and insert it into the `plugins` directory:
- ```
/usr/java/jdk1.5.0_08/bin/jar cvf ../ica-plugin.jar *
```
- Step 8**    In ASDM, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-in > Import**.
- Step 9**    Next to Plug-in Name, select **ica** to provide plug-in access to Citrix MetaFrame services.
- Step 10**   Click **Local computer**, click **Browse Local Files**, select the `ica-plugin.jar` file, then click **Select**.
- Step 11**   Click **Import Now**.
- Click **Apply**.
- The plug-in is now available for future Clientless SSL VPN sessions.

### Assembling and Installing Third-Party Plug-ins—Example: TN 5250 Client Plug-in

The open framework of the security appliance lets you add plug-ins to support third-party Java client/server applications. As an example of how to provide Clientless SSL VPN browser access to third-party plug-ins, this section describes how to add Clientless SSL VPN support for the MochaSoft W32 TN 5250 client.

**Caution**

Cisco does not provide direct support for or recommend any particular plug-ins that are not redistributed by Cisco. As a provider of Clientless SSL VPN services, you are responsible for reviewing and complying with any license agreements required for the use of plug-ins.

We provide a zip file within which you can insert the tn5250 client downloaded from MochaSoft. After you import the zip file as a plug-in into the security appliance, users can use the associated plug-in to emulate a 5250 terminal to connect to IBM mainframes over clientless SSL VPN sessions.

A stateful failover does not retain sessions established using plug-ins. Users must reauthenticate after a failover.

**Note**

You must follow the instructions in the [“Preparing the Security Appliance for a Plug-in” section on page 38-65](#) before proceeding, if you are not already providing support for a plug-in.

To install the TN 5250 plug-in, perform the following steps:

- 
- Step 1** Create a directory on your computer to store plug-ins. For example,  
C:\plugins
  - Step 2** Create a subdirectory to store files specific to the plug-in to be built. For example,  
C:\plugins\tn5250
  - Step 3** Download the tn5250-plugin.yymmdd.zip file from the Cisco ASA software download site to the new subdirectory.  
  
Cisco customized this file for use with the MochaSoft tn5250 plug-in.
  - Step 4** Go to <http://www.mochasoft.dk/download1java.htm> and download the mtn5250.zip file to the new subdirectory.
  - Step 5** Extract the tn5250.jar file and add it to the Cisco tn5250-plugin.yymmdd.zip file.  
  
For example, use WinZip to add the jar files to the zip file.
  - Step 6** In ASDM, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-in > Import**.
  - Step 7** Next to Plug-in Name, select **tn5250**.
  - Step 8** Click **Local computer**, click **Browse Local Files**, select the tn5250-plugin.yymmdd.zip file, then click **Select**.
  - Step 9** Click **Import Now**.
  - Step 10** Click **Apply**.  
  
The plug-in is now available for future Clientless SSL VPN sessions.
  - Step 11** (Optional) Add a bookmark entry (link) to a bookmark list so that users can click a link to establish a plug-in connection to the server.  
  
The URL of the bookmark must be in the following form: tn5250://domain\_name\_of\_host  
For example: tn5250://example\_domain
  - Step 12** (Required only if you followed step 11) Assign the bookmark list to the group policies, local user policies, or DAPs for whom you want to provide access.



- Step 13** To test the plug-in, establish a clientless SSL VPN session. Select the TN5250 menu option and enter the address using the syntax shown above, or click the bookmark.
- 

### Assembling and Installing Third-Party Plug-ins—Example: TN 3270 Client Plug-in

The open framework of the security appliance lets you add plug-ins to support third-party Java client/server applications. As an example of how to provide Clientless SSL VPN browser access to third-party plug-ins that are not redistributed by Cisco, this section describes how to add Clientless SSL VPN support for the MochaSoft W32 TN 3270 client.



#### Caution

Cisco does not provide direct support for or recommend any particular plug-ins that are not redistributed by Cisco. As a provider of Clientless SSL VPN services, you are responsible for reviewing and complying with any license agreements required for the use of plug-ins.

---

We provide a zip file within which you can insert the tn3270 client plug-in to be downloaded from MochaSoft. After you import the zip file as a plug-in into the security appliance, users can use the associated plug-in to emulate a 3270 terminal to connect to IBM mainframes over clientless SSL VPN sessions.

A stateful failover does not retain sessions established using plug-ins. Users must reauthenticate after a failover.



#### Note

You must follow the instructions in the [“Preparing the Security Appliance for a Plug-in”](#) section on [page 38-65](#) before proceeding, if you are not already providing support for a plug-in.

---

To install the TN 3270 plug-in, perform the following steps:

---

- Step 1** Create a directory on your computer to store plug-ins. For example,  
C:\plugins
- Step 2** Create a subdirectory to store files specific to the plug-in to be built. For example,  
C:\plugins\tn3270
- Step 3** Download the tn3270-plugin.yymmdd.zip file from the Cisco ASA software download site to the new subdirectory.  
  
Cisco customized this file for use with the MochaSoft tn3270 plug-in.
- Step 4** Go to <http://www.mochasoft.dk/download1java.htm> and download the mtn3270.zip file to the new subdirectory.
- Step 5** Extract the tn3270.jar file and add it to the tn3270-plugin.yymmdd.zip file.  
  
For example, use WinZip to add the jar files to the zip file.
- Step 6** In ASDM, choose **Config > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-in > Import**.
- Step 7** Next to Plug-in Name, select **tn3270**.
- Step 8** Click **Local computer**, click **Browse Local Files**, select the tn3270-plugin.yymmdd.zip file, then click **Select**.
- Step 9** Click **Import Now**.

- Step 10** Click **Apply**.  
The plug-in is now available for future Clientless SSL VPN sessions.
- Step 11** (Optional) Add a bookmark entry (link) to a bookmark list so that users can click a link to establish a plug-in connection to the server.  
The URL of the bookmark must be in the following form: tn3270://domain\_name\_of\_host  
For example: tn3270://example\_domain
- Step 12** (Required only if you followed step 11) Assign the bookmark list to the group policies, local user policies, or DAPs for whom you want to provide access.
- Step 13** To test the plug-in, establish a clientless SSL VPN session. Click the TN3270 menu option and enter the address using the syntax shown above, or click the bookmark.

## Language Localization

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, screens associated with optional plug-ins, and the interface displayed to Cisco AnyConnect VPN Client users.

This section describes how to configure the security appliance to translate these user messages and includes the following sections:

- [Understanding Language Translation, page 38-72](#)
- [Creating a Translation Table, page 38-73](#)
- [Add/Edit Localization Entry, page 38-74](#)
- [Import/Export Language Localization, page 38-77](#)

### Understanding Language Translation

Each functional area and its messages that are visible to remote users are organized into translation domains. [Table 38-6](#) shows the translation domains and the functional areas translated.

**Table 38-6 Translation Domains and Functional Areas Affected**

| Translation Domain   | Functional Areas Translated                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------|
| <b>AnyConnect</b>    | Messages displayed on the user interface of the Cisco AnyConnect VPN Client.                        |
| <b>CSD</b>           | Messages for the Cisco Secure Desktop (CSD).                                                        |
| <b>customization</b> | Messages on the logon and logout pages, portal page, and all the messages customizable by the user. |
| <b>keepout</b>       | Message displayed to remote users when VPN access is denied.                                        |
| <b>PortForwarder</b> | Messages displayed to Port Forwarding users.                                                        |
| <b>url-list</b>      | Text that user specifies for URL bookmarks on the portal page.                                      |
| <b>webvpn</b>        | All the layer 7, AAA and portal messages that are not customizable.                                 |
| <b>plugin-ica</b>    | Messages for the Citrix plug-in.                                                                    |
| <b>plugin-rdp</b>    | Messages for the Remote Desktop Protocol plug-in.                                                   |

| Translation Domain | Functional Areas Translated              |
|--------------------|------------------------------------------|
| plugin-telnet,ssh  | Messages for the Telnet and SSH plug-in. |
| plugin-vnc         | Messages for the VNC plug-in.            |

The software image package for the security appliance includes a language localization template for each domain that is part of the standard functionality. The templates for plug-ins are included with the plug-ins and define their own translation domains.

You can export the template for a translation domain, which creates an XML file of the template at the URL you provide. The message fields are empty in this file. You can customize the messages and import the template to create a new language localization table that resides in flash memory.

You can also export an existing language localization table. The XML file created displays the messages you edited previously. Reimporting this XML file with the same language name creates a new version of the language localization table, overwriting previous messages.

Some templates are static, but some change based on the configuration of the security appliance. Because you can customize the *logon and logout pages*, *portal page*, and *URL bookmarks for clientless sessions*, the **security appliance generates the customization** and **url-list** translation domain templates dynamically and the template automatically reflects your changes to these functional areas.

After creating language localization tables, they are available to customization objects that you create and apply to group policies or user attributes. A language localization table has no affect and messages are not translated on user screens until you create the customization object, identify a language localization table to use in that object, and specify the customization for the group policy or user.

### Fields

**Add**—Launches the Add Localization Entry dialog where you can select a localization template to add and you can edit the contents of the template.

**Edit**—Launches the Edit Localization Entry dialog for the selected language in the table, and allows you to edit the previously-imported language localization table.

**Delete**—Deletes a selected language localization table.

**Import**—Launches the Import Language Localization dialog where you can import a language localization template or table.

**Export**—Launches the Export Language Localization dialog where you can export a language localization template or table to a URL where you can make changes to the table or template.

**Language**—The language of existing Language Localization tables.

**Language Localization Template**—The template that the table is based on.

## Creating a Translation Table

The following procedure describes how to create a translation table:

- Step 1** Go to **Remove Access VPN > Clientless SSL VPN Access > Portal > Advanced > Language Localization**. The Language Localization pane displays. Click **Add**. The Add Language Localization window displays.
- Step 2** Select a Language Localization Template from the drop-down box. The entries in the box correspond to functional areas that are translated. For more information about the functionality for each template, see table [Table 38-6](#).

- Step 3** 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.
- Step 4** Edit the translation table. For each message represented by the msgid field that you want to translate, enter the translated text between the quotes of the associated msgstr field. The example below shows the message Connected, with the Spanish text in the msgstr field:
- ```
msgid "Connected"
msgstr "Conectado"
```
- Step 5** Click **OK**. The new table appears in the list of translation tables.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Add/Edit Localization Entry

You can add a new translation table, based on a template, or you can modify an already-imported translation table from this pane.

Fields

Language Localization Template—Select a template to modify and use as a basis for a new translation table. The templates are organized into translation domains and affect certain areas of functionality. The following table shows the translation domains and the functional areas affected:

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
keepout	Message displayed to remote users when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.

Language—Specify a language. Use an abbreviation that is compatible with the language options of your browser. The security appliance creates the new translation table with this name.

Text Editor—Use the editor to change the message translations. The message ID field (msgid) contains the default translation. The message string field (msgstr) that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string. For example, to translate the message “Connected” with a Spanish translation, insert the Spanish text between the msgstr quotes:

```
msgid "Connected"
msgstr "Conectado"
```

After making changes, click **Apply** to import the translation table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

AnyConnect Customization

Resources

Specify resource files that customize or re-brand the AnyConnect VPN client in this panel.



Note

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator's Guide and the release notes for the AnyConnect VPN Client.

Fields

Import—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

Export—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

Delete—Removes the selected object.

Platform—The type of remote PC platform supported by the object.

Object Name—The name of the object.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Binary

Specify third-party programs that use the AnyConnect VPN client API in this panel. The security appliance downloads these programs to the client for customizing the user interface or the command line interface.



Note

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator's Guide and the release notes for the AnyConnect VPN Client.

Fields

Import—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

Export—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

Delete—Removes the selected object.

Platform—The type of remote PC platform supported by the object.

Object Name—The name of the object.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Installs

Specify files for customizing the AnyConnect client installation in this panel.



Note

The security appliance does not support this feature for the AnyConnect VPN client, versions 2.0 and 2.1. For more information on manually customizing the client, see the AnyConnect VPN Client Administrator's Guide and the release notes for the AnyConnect VPN Client.

Fields

Import—Launches the Import AnyConnect Customization Objects dialog, where you can specify a file to import as an object.

Export—Launches the Export AnyConnect Customization Objects dialog, where you can specify a file to export as an object.

Delete—Removes the selected object.

Platform—The type of remote PC platform supported by the object.

Object Name—The name of the object.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Import/Export Language Localization

In the Import Translation Table and Export Translation Table windows you can import or export a translation table to the security appliance to provide translation of user messages.

Translation templates are XML files that contain message fields that can be edited with translated messages. You can export a template, edit the message fields, and import the template as a new translation table, or you can export an existing translation table, edit the message fields, and re-import the table to overwrite the previous version.

Fields

- **Language**—Enter a name for the language.

When *exporting*, it is automatically filled-in with the name from the entry you selected in the table.

When *importing*, you enter the language name in the manner that you want it to be identified. The imported translation table then appears in the list with the abbreviation you designated. To ensure that your browser recognizes the language, use language abbreviations that are compatible with the language options of the browser. For example, if you are using IE, use **zh** as the abbreviation for the Chinese language.

- **Localization Template Name**—The name of the XML file containing the message fields. The following templates are available:
 - AnyConnect—Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
 - CSD—Messages for the Cisco Secure Desktop (CSD).
 - customization—Messages on the logon and logout pages, portal page, and all the messages customizable by the user.
 - keepout—Message displayed to remote users when VPN access is denied.
 - PortForwarder—Messages displayed to Port Forwarding users.
 - url-list—Text that user specifies for URL bookmarks on the portal page.

- webvpn—All the layer 7, AAA and portal messages that are not customizable.
- plugin-ica—Messages for the Citrix plug-in.
- plugin-rdp—Messages for the Remote Desktop Protocol plug-in.
- plugin-telnet,ssh—Messages for the TELNET and SSH plug-in.
- plugin-vnc—Messages for the VNC plug-in.
- **Select a file**—Choose the method by which you want to import or export the file.
 - Remote server—Select this option to import a customization file that resides on a remote server accessible from the security appliance.
 - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - Flash file system—Choose this method to export a file that resides on the security appliance.
 - Path—Provide the path to the file.
 - Browse Flash—Browse to the path for the file.
 - Local computer—Choose this method to import a file that resides on the local PC.
 - Path—Provide the path to the file.
 - Browse Local Files—Browse to the path for the file.
- **Import/Export Now**—Click to import or export the file.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Configure GUI Customization Objects (Bookmark Lists)

This dialog box lets you add, edit, and delete, import and export bookmark lists.

The Bookmarks window lets you configure lists of servers and URLs for access over clientless SSL VPN. Following the configuration of a bookmark list, you can assign the list to one or more usernames, group policies, and DAPs. Each username, group policy, and DAP can have only one bookmark list. The list names populate a drop-down list on the URL Lists tab of each DAP.

Version 8.0 software extends the functionality for configuring bookmark lists, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new lists. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.



Note

Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file *before* you upgrade to Version 8.0.

Fields

- Bookmarks—Displays the existing bookmark lists.
- Add—Click to add a new bookmark list.
- Edit—Click to edit the selected bookmark list.
- Delete—Click to delete the selected bookmark list.
- Import—Click to import a bookmark list.
- Export—Click to export a bookmark list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Bookmark List

The Add/Edit Bookmark List dialog box configure lists of servers and URLs for access over lets you add, edit, or delete a URL list, and also order the items in a designated URL list.

Fields

- Bookmark List Name—Specifies the name of the list to be added or selects the name of the list to be modified or deleted.
- Bookmark Title—Specifies the URL name displayed to the user.
- URL—Specifies the actual URL associated with the display name.
- Add—Opens the Add Bookmark Entry dialog box, on which you can configure a new server or URL and display name.
- Edit—Opens the Edit Bookmark Entry dialog box, on which you can configure a new server or URL and display name.
- Delete—Removes the selected item from the URL list. There is no confirmation or undo.
- Move Up/Move Down—Changes the position of the selected item in the URL list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add Bookmark Entry

The Add Bookmark Entry dialog box lets you create a link or bookmark for a URL list.

Fields

- **Bookmark Title**—Enter a name for the bookmark to display for the user.
- **URL (drop-down)**—Use the pull-down menu to select the URL type: http, https, cifs, or ftp. The URL types of all imported plug-ins also populate this menu. Select the URL type of a plug-in if you want to display the plug-in as a link on the portal page.
- **URL (text box)**—Enter the DNS name or IP address for the bookmark. For a plug-in, enter the name of the server. Enter a forward slash and a question mark (/?) after the server name to specify optional parameters, then use an ampersand to separate parameter-value pairs, as shown in the following syntax:

server/?Parameter=Value&Parameter=Value

For example:

host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

The particular plug-in determines the optional parameter-value pairs that you can enter.

To provide single sign-on support for a plug-in, use the parameter-value pair **cscsso=1**. For example:

host/?cscsso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

- **Subtitle**—Provide additional user-visible text that describes the bookmark entry.
- **Thumbnail**—Use the pull-down menu to select an icon to associate with the bookmark on the end-user portal.
- **Manage**—Click to import or export images to use as thumbnails.
- **Enable Smart Tunnel Option**—Select to open the bookmark in a new window that uses the smart tunnel feature to pass data through the security appliance to or from the destination server. This option lets you provide smart tunnel support for a browser-based application, whereas the Smart Tunnels option, also in the Clientless SSL VPN > Portal menu, lets you add nonbrowser-based applications to a smart tunnel list for assignment to group policies and usernames.
- **Allow the users to bookmark the link**—Check to let clientless SSL VPN users use the Bookmarks or Favorites options on their browsers. Uncheck to prevent access to these options.
- **Advanced Options**—(Optional) Open to configure further bookmark characteristics.
 - **URL Method**—Select Get for simple data retrieval. Choose Post when processing the data might involve changes to it, for example, storing or updating data, ordering a product, or sending e-mail.
 - **Post Parameters**—Configure the particulars of the Post URL method.
 - **Add/Edit**—Click to add a post parameter.
 - **Edit**—Click to edit the highlighted post parameter.
 - **Delete**—Click to delete the highlighted post parameter.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Import/Export Bookmark List

You can import or export already configured bookmark lists. Import lists that are ready to use. Export lists to modify or edit them, and then reimport.

Fields

- **Bookmark List Name**—Identify the list by name. Maximum 64 characters, no spaces.
- **Select a file**—Choose the method by which you want to import or export the list file.
 - **Local computer**—Select to import a file that resides on the local PC.
 - **Flash file system**—Select to export a file that resides on the security appliance.
 - **Remote server**—Select to import a url list file that resides on a remote server accessible from the security appliance.
 - **Path**—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - **Browse Local Files/Browse Flash**—Browse to the path for the file.
- **Import/Export Now**—Click to import or export the list file.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Configure GUI Customization Objects (Web Contents)

This dialogue box lets you import and export web content objects.

Fields

- **File Name**—Displays the names of the web content objects.
- **File Type**—Identifies the file type(s).
- **Import/Export**—Click to import or export a web content object.
- **Delete**—Click to delete the object.

Import/Export Web Content

Web contents can range from a wholly configured home page to icons or images you want to use when you customize the end user portal. You can import or export already configured web contents. Import web contents that are ready for use. Export web contents to modify or edit them, and then reimport.

Fields

- Source—Choose the location from which you want to import or export the file.
 - Local computer—Select to import or export a file that resides on the local PC.
 - Flash file system—Select to import or export a file that resides on the security appliance.
 - Remote server—Select to import a file that resides on a remote server accessible from the security appliance.
 - Path—Identify the method to access the file (ftp, http, or https), and provide the path to the file.
 - Browse Local Files.../Browse Flash...—Browse to the path for the file.
- Destination
 - Require authentication to access its content? Click Yes or No.
 - WebContent Path: Notice that the prefix to the path changes depending on whether you require authentication. The security appliance uses /+CSCOE+/ for objects that require authentication, and /+CSCOU+/ for objects that do not. The security appliance displays /+CSCOE+/ objects on the portal page only, while /+CSCOU+/ objects are visible and usable in either the logon or the portal pages.
- Import/Export Now—Click to import or export the file.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Add/Edit Post Parameter

Use this pane to configure post parameters for bookmark entries and URL lists.

Since these are often personalized resources that contain the user ID and password or other input parameters, you might need to define [Clientless SSL VPN Macro Substitutions](#). Click the link for detailed instructions.

Fields

- Name, Value—Provide the name and value of the parameters exactly as in the corresponding HTML form, for example: `<input name="param_name" value="param_value">`.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Clientless SSL VPN Macro Substitutions

Clientless SSL VPN macro substitutions let you configure users for access to personalized resources that contain the user ID and password or other input parameters. Examples of such resources include bookmark entries, URL lists, and file shares.



Note

For security reasons, password substitutions are disabled for file access URLs (cifs://).

Also for security reasons, use caution when introducing password substitutions for web links, especially for non-SSL instances.

We support the following macro substitutions:

No.	Macro Substitution	Definition
1	CSCO_WEBVPN_USERNAME	SSL VPN user login ID
2	CSCO_WEBVPN_PASSWORD	SSL VPN user login password
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN user internal resource password
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN user login group drop-down, a group alias within the connection profile
5	CSCO_WEBVPN_MACRO1	Set via RADIUS/LDAP vendor-specific attribute
6	CSCO_WEBVPN_MACRO2	Set via RADIUS/LDAP vendor-specific attribute

Using Macros 1 - 4

The security appliance obtains values for the first four substitutions from the SSL VPN Login page, which includes fields for username, password, internal password (optional), and group. It recognizes these strings in user requests, and replaces them with the value specific to the user before it passes the request on to a remote server.

For example, if a URL list contains the link, http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the security appliance translates it to the following unique links:

- For USER1 the link becomes <http://someserver/homepage/USER1.html>
- For USER2 the link is <http://someserver/homepage/USER2.html>

In the following case, cifs://server/users/CSCO_WEBVPN_USERNAME, lets the security appliance map a file drive to specific users:

- For USER1 the link becomes <cifs://server/users/USER1>
- For USER2 the link is <cifs://server/users/USER2>

Using Macros 5 and 6

Values for macros 5 and 6 are RADIUS or LDAP vendor-specific attributes (VSAs). These substitutions let you set substitutions configured on either a RADIUS or an LDAP server.

Example 1: Setting a Homepage

The following example sets a URL for the homepage:

- WebVPN-Macro-Value1 (ID=223), type string, is returned as *wwwin-portal.abc.com*
- WebVPN-Macro-Value2 (ID=224), type string, returned as *401k.com*

To set a home page value, you would configure the macro as

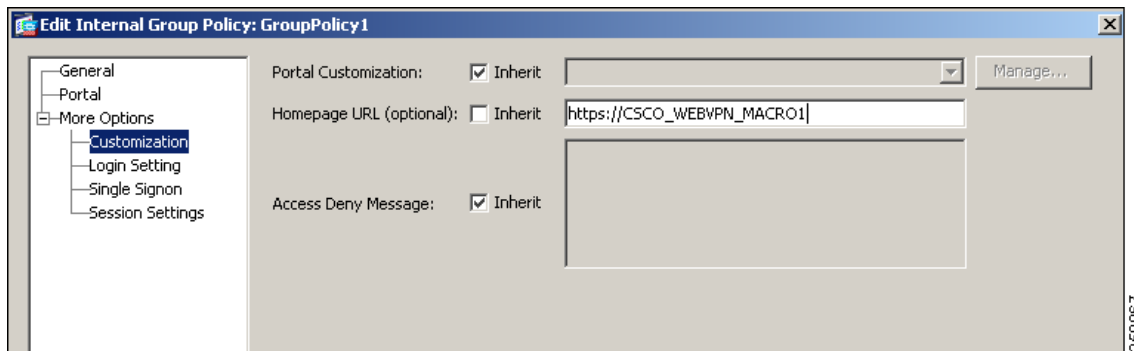
`https://CSCO_WEBVPN_MACRO1`, which would translate to <https://wwwin-portal.abc.com>.

The best way to do this is to configure the Homepage URL parameter in ASDM.

Go to the Add/Edit Group Policy pane, from either the Network Client SSL VPN or Clientless SSL VPN Access section of ASDM, as in [Figure 38-1 Using ASDM to Configure a Macro that Sets a Homepage](#). The paths are as follows:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > SSL VPN Client > Customization > Homepage URL attribute.
- Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > More Options > Customization > Homepage URL attribute.

Figure 38-1 Using ASDM to Configure a Macro that Sets a Homepage



Example 2: Setting a Bookmark or URL Entry

You can use an HTTP Post to log in to an OWA resource using an RSA one-time password (OTP) for SSL VPN authentication, and then the static, internal password for OWA e-mail access. The best way to do this is to add or edit a bookmark entry in ASDM, as in [Figure 38-2 Configuring a Bookmark Entry](#).

There are several paths to the Add Bookmark Entry pane, including the following:

- Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add/Edit Bookmark Lists > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters (available after you click **Post** in the URL Method attribute).
- Configuration > Remote Access VPN > Clientless SSL VPN Access

or

(Available after you click **Post** in the URL Method attribute):

Network (Client) Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > URL Lists tab > Manage button > Configured GUI Customization Objects > Add/Edit button > Add/Edit Bookmark List > Add/Edit Bookmark Entry > Advanced Options area > Add/Edit Post Parameters

Figure 38-2 Configuring a Bookmark Entry

Add Bookmark Entry

Bookmark Title: Web e-mail

URL Value: https://mail.abc.com/exchweb/bin/auth/owaauth.dll

Advanced Options

Subtitle:

Thumbnail: -- None -- Manage

URL Method : ☐ Get ☒ Post

Enable Favorite Option: ☒ Yes ☐ No

Enable Smart Tunnel Option: ☐ Yes ☒ No

Post Parameters

Add Edit Delete

Name	Value
destination	https://email.abc.com/xchange
flags	0
username	CSCO_WEBVPN_USERNAME
password	CSCO_WEBVPN_INTERNAL_PASSWORD
SubmitCredentials	Log On

OK Cancel Help

250066



CHAPTER 39

E-Mail Proxy

E-mail proxies extend remote e-mail capability to users of Clientless SSL VPN. When users attempt an e-mail session via e-mail proxy, the e-mail client establishes a tunnel using the SSL protocol.

The e-mail proxy protocols are as follows:

POP3S

POP3S is one of the e-mail 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 establishes, the POP3 protocol starts, and then authentication occurs. POP3S is for receiving e-mail.

IMAP4S

IMAP4S is one of the e-mail 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 establishes, the IMAP4 protocol starts, and then authentication occurs. IMAP4S is for receiving e-mail.

SMTPS

SMTPS is one of the e-mail 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 e-mail.

Configuring E-Mail Proxy

Configuring e-mail proxy on the consists of the following tasks:

- Enabling e-Mail proxy on interfaces.
- Configuring e-mail proxy default servers.
- Setting AAA server groups and a default group policy.
- Configuring delimiters.

Configuring E-mail proxy also has these requirements:

- Users who access e-mail from both local and remote locations via e-mail proxy require separate e-mail accounts on their e-mail program for local and remote access.
- E-mail proxy sessions require that the user authenticate.

AAA

Configuration > Remote Access VPN > Advanced > E-mail Proxy > AAA

Select the [AAA server groups](#) and default [group policies](#) for E-mail Proxy.

POP3S | IMAP4S | SMTPS

Authentication Server Group: RADIUS

Authorization Server Group: -- None --

☐ Users must exist in the authorization database to connect

Accounting Server Group: -- None --

Default Group Policy: DfltGrpPolicy

Authorization Settings

☐ Use the entire DN as the username

☒ Specify individual DN fields as the username:

Primary DN Field: Common Name (CN)

Secondary DN Field: Organizational Unit (OU)

Apply Reset

This panel has three tabs:

- [POP3S Tab](#)
- [IMAP4S Tab](#)
- [SMTPS Tab](#)

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

POP3S Tab

The POP3S AAA panel associates AAA server groups and configures the default group policy for POP3S sessions.

Fields

- **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 POP3S user authentication. The default is to have no authentication servers configured. If you have set AAA as the authentication method for POP3S (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel), you must configure an AAA server and select it here, or authentication always fails.
- **Authorization Server Group**—Select the authorization server group for POP3S user authorization. The default is to have no authorization servers configured.
- **Accounting Server Group**—Select the accounting server group for POP3S user accounting. The default is to have no accounting servers configured.
- **Default Group Policy**—Select the group policy to apply to POP3S 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 security appliance can not establish the session.
- **Authorization Settings**—Lets you set values for usernames that the security appliance recognizes for POP3S authorization. This applies to POP3S users that authenticate with digital certificates and require LDAP or RADIUS authorization.
 - **User the entire DN as the username**—Select to use the Distinguished Name for POP3S 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 e-mail address. Then a user with the Common Name (CN) John Doe and an e-mail 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 Does must authenticate as johndoe@cisco.com and Cisco Systems, Inc.
 - **Primary DN Field**—Select the primary DN field you want to configure for POP3S 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 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.
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.

DN Field**Definition**

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 you want to configure for POP3S authorization. The default is OU. Options include all of those in the preceding table, with the addition of **None**, which you select if you do not want to include a secondary field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

IMAP4S Tab

The IMAP4S AAA panel associates AAA server groups and configures the default group policy for IMAP4S sessions.

Fields

- 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 policy—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 IMAP4S user authentication. The default is to have no authentication servers configured. If you have set AAA as the authentication method for IMAP4S (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel), you must configure an AAA server and select it here, or authentication always fails.
- Authorization Server Group—Select the authorization server group for IMAP4S user authorization. The default is to have no authorization servers configured.
- Accounting Server Group—Select the accounting server group for IMAP4S user accounting. The default is to have no accounting servers configured.

- **Default Group Policy**—Select the group policy to apply to IMAP4S users when AAA does not return a CLASSID attribute. If you do not specify a default group policy, and there is no CLASSID, the security appliance can not establish the session.
- **Authorization Settings**—Lets you set values for usernames that the security appliance recognizes for IMAP4S authorization. This applies to IMAP4S users that authenticate with digital certificates and require LDAP or RADIUS authorization.
 - **User the entire DN as the username**—Select to use the fully qualified domain name for IMAP4S 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 e-mail address. Then a user with the Common Name (CN) John Doe and an e-mail 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 Does must authenticate as johndoe@cisco.com *and* Cisco. Systems, Inc.
 - **Primary DN Field**—Select the primary DN field you want to configure for IMAP4S 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 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.
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 you want to configure for IMAP4S authorization. The default is OU. Options include all of those in the preceding table, with the addition of None, which you select if you do not want to include a secondary field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SMTPS Tab

The SMTPS AAA panel associates AAA server groups and configures the default group policy for SMTPS sessions.

Fields

- 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 policy—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 SMTPS user authentication. The default is to have no authentication servers configured. If you have set AAA as the authentication method for SMTPS (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel), you must configure an AAA server and select it here, or authentication always fails.
- Authorization Server Group—Select the authorization server group for SMTPS user authorization. The default is to have no authorization servers configured.
- Accounting Server Group—Select the accounting server group for SMTPS user accounting. The default is to have no accounting servers configured.
- Default Group Policy—Select the group policy to apply to SMTPS users when AAA does not return a CLASSID attribute. If you do not specify a default group policy, and there is no CLASSID, the security appliance can not establish the session.
- Authorization Settings—Lets you set values for usernames that the security appliance recognizes for SMTPS authorization. This applies to SMTPS users that authenticate with digital certificates and require LDAP or RADIUS authorization.
 - User the entire DN as the username—Select to use the fully qualified domain name for SMTPS 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 e-mail address. Then a user with the Common Name (CN) John Doe and an e-mail 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 Does must authenticate as johndoe@cisco.com *and* Cisco. Systems, Inc.

- **Primary DN Field**—Select the primary DN field you want to configure for SMTPS 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 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.
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 you want to configure for SMTPS authorization. The default is OU. Options include all of those in the preceding table, with the addition of None, which you select if you do not want to include a secondary field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Access

The E-mail Proxy Access screen lets you identify interfaces on which to configure e-mail proxy. You can configure and edit e-mail proxies on individual interfaces, and you can configure and edit e-mail proxies for one interface and then apply your settings to all interfaces. You cannot configure e-mail proxies for management-only interfaces, or for subinterfaces.

Configuration > Remote Access VPN > Advanced > E-mail Proxy > Access E-Mail Proxy

Enable e-mail proxy functionality at the interface level.

Interface	POP3S Enabled	IMAP4S Enabled	SMTPS Enabled	Edit
DMZ	No	No	No	
dmz1	No	No	No	
inside	No	No	No	
outside	No	No	No	

Apply Reset

191695

Fields

- 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.
- Edit—Click to edit the e-mail proxy settings for the highlighted interface.

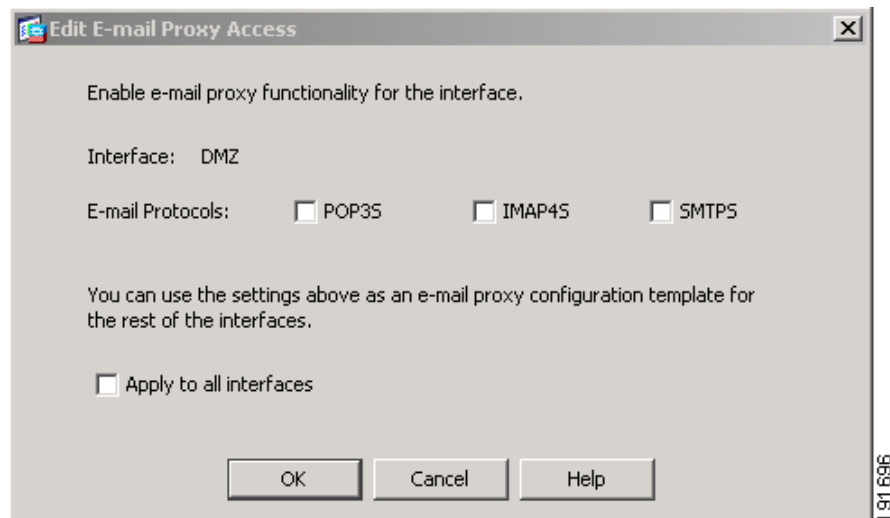
Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Edit E-Mail Proxy Access

The E-mail Proxy Access screen lets you identify interfaces on which to configure e-mail proxy. You can configure e-mail proxies on individual interfaces, and you can configure e-mail proxies for one interface and then apply your settings to all interfaces.



Fields

- Interface—Displays the name of the selected interface.
- POP3S Enabled—Select to enable POP3S for the interface.
- IMAP4S Enabled—elect to enable IMAP4S for the interface.
- SMTPS Enabled—Select to enable SMTPS for the interface.
- Apply to all interface—Select to apply the settings for the current interface to all configured interfaces.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Authentication

This panel lets you configure authentication methods for e-mail proxy sessions.

Configuration > Remote Access VPN > Advanced > E-mail Proxy > Authentication

Configure e-mail proxy authentication. Mailhost authentication is always performed for POP3S and IMAP4S.

POP3S Authentication

☐ AAA ☐ Piggyback HTTPS

☐ Certificate

IMAP4S Authentication

☐ AAA ☐ Piggyback HTTPS

☐ Certificate

SMTPS Authentication

☒ AAA ☐ Piggyback HTTPS

☐ Certificate ☐ Mailhost

Apply Reset

191697

Fields

POP3S/IMAP4S/SMTPS Authentication—Let you configure authentication methods for each of the e-mail proxy types. You can select 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 e-mail username, separated by the VPN Name Delimiter, only if the usernames are different from each other.
- **Certificate**—Certificate authentication does not work for e-mail proxies in the current security appliance software release.
- **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 e-mail username only. No password is required. Users must present both the VPN username and the e-mail username, separated by the VPN Name Delimiter, only if the usernames are different from each other.

SMTPS e-mail 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 security appliance, 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 e-mail 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 e-mail username, server and password.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Default Servers

This panel lets you identify proxy servers to the security appliance. Enter the IP address and port of the appropriate proxy server.

Configuration > Remote Access VPN > Advanced > E-mail Proxy > Default Servers

Configure default e-mail server settings.

POP3S Default Server

Name or IP Address:

Port: ☒ Enable non-authenticated session limit:

IMAP4S Default Server

Name or IP Address:

Port: ☒ Enable non-authenticated session limit:

SMTPS Default Server

Name or IP Address:

Port: ☒ Enable non-authenticated session limit:

Apply Reset

Fields

- **POP3S/IMAP4S/SMTPS Default Server**—Let you configure a default server, port and non-authenticated session limit for e-mail proxies.
- **Name or IP Address**—Type the DNS name or IP address for the default e-mail proxy server.
- **Port**—Type the port number on which the security appliance listens for e-mail proxy traffic. Connections are automatically allowed to the configured port. The e-mail proxy allows only SSL connections on this port. After the SSL tunnel establishes, the e-mail proxy starts, and then authentication occurs.

For POP3s the default port is 995, for IMAP4S it is 993, and for SMTPS it is 988.

- **Enable non-authenticated session limit**—Select to restrict the number of non-authenticated e-mail proxy sessions.

E-mail proxy connections have three states:

1. A new e-mail connection enters the “unauthenticated” state.
2. When the connection presents a username, it enters the “authenticating” state.
3. When the security appliance authenticates the connection, it enters the “authenticated” state.

This feature lets you set a limit for sessions in the process of authenticating, thereby preventing DOS attacks. When a new session exceeds the set limit, the security appliance terminates the oldest non-authenticating connection. If there are no non-authenticating connections, the oldest authenticating connection is terminated. The does not terminate authenticated sessions.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Delimiters

This panel lets you configure username/password delimiters and server delimiters for e-mail proxy authentication.

Configuration > Remote Access VPN > Advanced > E-mail Proxy > Delimiters

Configure the username/password and server delimiters. The delimiters for the same protocol must be different.

POP3S Delimiters

Username/Password Delimiter: Colon (:)

Server Delimiter: At (@)

IMAP4S Delimiters

Username/Password Delimiter: Colon (:)

Server Delimiter: At (@)

SMTPS Delimiters

Username/Password Delimiter: Colon (:)

Server Delimiter: At (@)

Apply Reset

66919

Fields

- **POP3S/IMAP4S/SMTPS Delimiters**—Let you configure username/password and server delimiters for each of the e-mail proxies.
 - **Username/Password Delimiter**—Select a delimiter to separate the VPN username from the e-mail username. Users need both usernames when using AAA authentication for e-mail proxy and the VPN username and e-mail username are different. Users enter both usernames, separated by the delimiter you configure here, and also the e-mail server name, when they log in to an e-mail proxy session.

**Note**

Passwords for Clientless SSL VPN e-mail proxy users cannot contain characters that are used as delimiters.

- **Server Delimiter**—Select a delimiter to separate the username from the name of the e-mail 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 e-mail proxy session.

For example, using : as the VPN Name Delimiter and @ as the Server Delimiter, when logging in to an e-mail program via e-mail proxy, the user would enter their username in the following format: vpn_username:e-mail_username@server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—



CHAPTER 40

Configuring SSL Settings

SSL

The security appliance uses the Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS) to achieve secure message transmission for both ASDM and Clientless, browser-based sessions. The SSL window lets you configure SSL versions for clients and servers and encryption algorithms. It also lets you apply previously configured trustpoints to specific interfaces, and to configure a fallback trustpoint for interfaces that do not have an associated trustpoint.

Fields

- **Server SSL Version**—Choose to specify the SSL/TLS protocol version the security appliance uses to negotiate as a server. You can make only one selection.

Options for Server SSL versions include the following:

Any	The security appliance accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
Negotiate SSL V3	The security appliance accepts SSL version 2 client hellos, and negotiates to SSL version 3.
Negotiate TLS V1	The security appliance accepts SSL version 2 client hellos, and negotiates to TLS version 1.
SSL V3 Only	The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3.
TLS V1 Only	The security appliance accepts only TLSv1 client hellos, and uses only TLS version 1.



Note

To use port forwarding for Clientless SSL VPN, you must select Any or Negotiate SSL V3. The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

- **Client SSL Version**—Choose to specify the SSL/TLS protocol version the security appliance uses to negotiate as a client. You can make only one selection.

Options for Client SSL versions include the following:

any	The security appliance sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1.
ssl3-only	The security appliance sends SSL version 3 hellos, and accepts only SSL version 3.
tlsv1-only	The security appliance sends TLSv1 client hellos, and accepts only TLS version 1.

- **Encryption**—Lets you set SSL encryption algorithms.
 - **Available Algorithms**—Lists the encryption algorithms the security appliance supports that are not in use for SSL connections. To use, or make active, an available algorithm, highlight the algorithm and click **Add**.
 - **Active Algorithms**—Lists the encryption algorithms the security appliance supports and is currently using for SSL connections. To discontinue using, or change an active algorithm to available status, highlight the algorithm and click **Remove**.
 - **Add/Remove**—Click to change the status of encryption algorithms in either the Available or Active Algorithms columns.
 - **Move Up/Move Down**—Highlight an algorithm and click these buttons to change its priority. The security appliance attempts to use an algorithm
- **Certificates**—Lets you select a fallback certificate, and displays configured interfaces and the configured certificates associated with them.
 - **Fallback Certificate**—Click to select a certificate to use for interfaces that have no certificate associated with them. If you select **None**, the security appliance uses the default RSA key-pair and certificate.
 - **Interface and ID Certificate** columns—Display configured interfaces and the certificate, if any, for the interface.
 - **Edit**—Click to change the trustpoint for the highlighted interface.
- **Apply**—Click to apply your changes.
- **Reset**—Click to remove changes you have made and reset SSL parameters to the values that they held when you opened the window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit SSL Certificate

Fields

- **Interface**—Displays the name of the interface you are editing.

- **Certificate**—Click to select a previously enrolled certificate to associate with the named interface.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SSL Certificates

In this pane, you can require that device management sessions require user certificates for SSL authentication.

Fields

- **Interface**—Displays the name of the interface you are editing.
- **User Certificate Required**—Click to select a previously enrolled certificate to associate with the named interface.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—



PART 5

Monitoring the Security Appliance



CHAPTER 41

Monitoring Interfaces

ASDM lets you monitor interface statistics as well as interface-related features.

ARP Table

The ARP Table pane displays the ARP table, including static and dynamic entries. The ARP table includes entries that map a MAC address to an IP address for a given interface. See Configuration > Properties > [ARP Static Table](#) for more information about the ARP table.

Fields

- Interface—Lists the interface name associated with the mapping.
- IP Address—Shows the IP address.
- MAC Address—Shows the MAC address.
- Proxy ARP—Displays Yes if proxy ARP is enabled on the interface. Displays No if proxy ARP is not enabled on the interface.
- Clear—Clears the dynamic ARP table entries. Static entries are not cleared.
- Refresh—Refreshes the table with current information from the security appliance and updates Last Updated date and time.
- Last Updated—*Display only*. Shows the date and time the display was updated.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DHCP

The security appliance lets you monitor DHCP status, including the addresses assigned to clients, the lease information for a security appliance interface, and DHCP statistics.

DHCP Server Table

The DHCP Server Table lists the IP addresses assigned to DHCP clients.

Fields

- IP Address—Shows the IP address assigned to the client.
- Client-ID—Shows the client MAC address or ID.
- Lease Expiration—Shows the date that the DHCP lease expires. The lease indicates how long the client can use the assigned IP address. Remaining time is also specified in the number of seconds and is based on the timestamp in the Last Updated display-only field.
- Number of Active Leases—Shows the total number of DHCP leases.
- Refresh—Refreshes the information from the security appliance.
- Last Updated—Shows when the data in the table was last updated.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DHCP Client Lease Information

If you obtain the security appliance interface IP address from a DHCP server, the DHCP Client Lease Information panel shows information about the DHCP lease.

Fields

- Select an interface—Lists the security appliance interfaces. Choose the interface for which you want to view the DHCP lease. If an interface has multiple DHCP leases, then choose the interface and IP address pair you want to view.
- Attribute and Value—Lists the attributes and values of the interface DHCP lease.
 - Temp IP addr—*Display only*. The IP address assigned to the interface.
 - Temp sub net mask—*Display only*. The subnet mask assigned to the interface.
 - DHCP lease server—*Display only*. The DHCP server address.
 - state—*Display only*. The state of the DHCP lease, as follows:
 - Initial—The initialization state, where the security appliance begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails.
 - Selecting—The security appliance is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one.
 - Requesting—The security appliance is waiting to hear back from the server to which it sent its request.
 - Purging—The security appliance is removing the lease because of an error.

Bound—The security appliance has a valid lease and is operating normally.

Renewing—The security appliance is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply.

Rebinding—The security appliance failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends.

Holddown—The security appliance started the process to remove the lease.

Releasing—The security appliance sends release messages to the server indicating that the IP address is no longer needed.

- **Lease**—*Display only*. The length of time, specified by the DHCP server, that the interface can use this IP address.
- **Renewal**—*Display only*. The length of time until the interface automatically attempts to renew this lease.
- **Rebind**—*Display only*. The length of time until the security appliance attempts to rebind to a DHCP server. Rebinding occurs if the security appliance cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The security appliance then attempts to contact any available DHCP server by broadcasting DHCP requests.
- **Next timer fires after**—*Display only*. The number of seconds until the internal timer triggers.
- **Retry count**—*Display only*. If the security appliance is attempting to establish a lease, this field shows the number of times the security appliance tried sending a DHCP message. For example, if the security appliance is in the Selecting state, this value shows the number of times the security appliance sent discover messages. If the security appliance is in the Requesting state, this value shows the number of times the security appliance sent request messages.
- **Client-ID**—*Display only*. The client ID used in all communication with the server.
- **Proxy**—*Display only*. Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
- **Hostname**—*Display only*. The client hostname.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DHCP Statistics

The DHCP Statistics pane shows statistics for the DHCP server feature.

Fields

- **Message Type**—Lists the DHCP message types sent or received:
 - BOOTREQUEST
 - DHCPDISCOVER

- DHCPREQUEST
- DHCPDECLINE
- DHCPRELEASE
- DHCPINFORM
- BOOTREPLY
- DHCPOFFER
- DHCPACK
- DHCPNAK
- Count—Shows the number of times a specific message was processed.
- Direction—Shows if the message type is Sent or Received.
- Total Messages Received—Shows the total number of messages received by the security appliance.
- Total Messages Sent—Shows the total number of messages sent by the security appliance.
- Counter—Shows general statistical DHCP data, including the following:
 - DHCP UDP Unreachable Errors
 - DHCP Other UDP Errors
 - Address Pools
 - Automatic Bindings
 - Expired Bindings
 - Malformed Messages
- Value—Shows the number of each counter item.
- Refresh—Updates the DHCP table listings.
- Last Updated—Shows when the data in the tables was last updated.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

MAC Address Table

The MAC Address Table pane shows the static and dynamic MAC address entries. See Configuration > Properties > Bridging > [MAC Address Table](#) for more information about the MAC address table and adding static entries.

Fields

- Interface—Shows the interface name associated with the entry.
- MAC Address—Shows the MAC address.

- **Type**—Shows if the entry is static or dynamic.
- **Age**—Shows the age of the entry, in minutes. To set the timeout, see [MAC Address Table](#).
- **Refresh**—Refreshes the table with current information from the security appliance.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

Dynamic ACLs

The Dynamic ACLs pane shows a table of the Dynamic ACLs, which are functionally identical to the user-configured ACLs except that they are created, activated and deleted automatically by the security appliance. These ACLs do not show up in the configuration and are only visible in this table. They are identified by the “(dynamic)” keyword in the ACL header.

When you choose an ACL in this table, the contents of the ACL is shown in the bottom text field.

Fields

- **ACL**—Shows the name of the dynamic ACL.
- **Element Count**—Shows the number of elements in the ACL
- **Hit Count**—Shows the total hit count for all of the elements in the ACL.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Interface Graphs

The Interface Graphs pane lets you view interface statistics in graph or table form. If an interface is shared among contexts, the security appliance shows only statistics for the current context. The number of statistics shown for a subinterface is a subset of the number of statistics shown for a physical interface.

Fields

- Available Graphs for—Lists the types of statistics available for monitoring. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.
 - Byte Counts—Shows the number of bytes input and output on the interface.
 - Packet Counts—Shows the number of packets input and output on the interface.
 - Packet Rates—Shows the rate of packets input and output on the interface.
 - Bit Rates—Shows the bit rate for the input and output of the interface.
 - Drop Packet Count—Shows the number of packets dropped on the interface.

These additional statistics display for physical interfaces:

- Buffer Resources—Shows the following statistics:
 - Overruns—The number of times that the security appliance was incapable of handing received data to a hardware buffer because the input rate exceeded the security appliance capability to handle the data.
 - Underruns—The number of times that the transmitter ran faster than the security appliance could handle.
 - No Buffer—The number of received packets discarded because there was no buffer space in the main system. Compare this with the ignored count. Broadcast storms on Ethernet networks are often responsible for no input buffer events.
- Packet Errors—Shows the following statistics:
 - CRC—The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the security appliance notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
 - Frame—The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
 - Input Errors—The number of total input errors, including the other types listed here. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the other types.
 - Runts—The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
 - Giants—The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
 - Deferred—For FastEthernet interfaces only. The number of frames that were deferred before transmission due to activity on the link.
- Miscellaneous—Shows statistics for received broadcasts.
- Collision Counts—For FastEthernet interfaces only. Shows the following statistics:
 - Output Errors—The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.

Collisions—The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.

Late Collisions—The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.

- **Input Queue**—Shows the number of packets in the input queue, the current and the maximum, including the following statistics:

Hardware Input Queue—The number of packets in the hardware queue.

Software Input Queue—The number of packets in the software queue.

- **Output Queue**—Shows the number of packets in the output queue, the current and the maximum, including the following statistics:

Hardware Output Queue—The number of packets in the hardware queue.

Software Output Queue—The number of packets in the software queue.

- **Drop Packet Queue**—Shows the number of packets dropped.
- **Add**—Adds the selected statistic type to the selected graph window.
- **Remove**—Removes the selected statistic type from the selected graph window. This button name changes to Delete if the item you are removing was added from another panel, and is not being returned to the Available Graphs pane.
- **Show Graphs**—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, choose the open graph window name. The statistics already included on the graph are shown in the Selected Graphs pane, to which you can add additional types. Graph windows are named for ASDM followed by the interface IP address and the name “Graph”. Subsequent graphs are named “Graph (2)” and so on.
- **Selected Graphs**—Shows the statistic types you want to show in the selected graph window. You can include up to four types.
 - **Show Graphs**—Shows the graph window or updates the graph with additional statistic types if added.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Graph/Table

The Graph window shows a graph for the selected statistics. The Graph window can show up to four graphs and tables at a time. By default, the graph or table displays the real-time statistics. If you enable [History Metrics, page 6-6](#), you can view statistics for past time periods.

Fields

- View—Sets the time period for the graph or table. To view any time period other than real-time, enable [History Metrics, page 6-6](#). The data is updated according to the specification of the following options:
 - Real-time, data every 10 sec
 - Last 10 minutes, data every 10 sec
 - Last 60 minutes, data every 1 min
 - Last 12 hours, data every 12 min
 - Last 5 days, data every 2 hours
- Export—Exports the graph in comma-separated value format. If there is more than one graph or table on the Graph window, the Export Graph Data dialog box appears. Choose one or more of the graphs and tables listed by checking the box next to the name.
- Print—Prints the graph or table. If there is more than one graph or table on the Graph window, the Print Graph dialog box appears. Choose the graph or table you want to print from the Graph/Table Name list.
- Bookmark—Opens a browser window with a single link for all graphs and tables on the Graphs window, as well as individual links for each graph or table. You can then copy these URLs as bookmarks in your browser. ASDM does not have to be running when you open the URL for a graph; the browser launches ASDM and then displays the graph.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

PPPoE Client

The PPPoE Client Lease Information pane displays information about current PPPoE connections.

Fields

Select a PPPoE interface—Select an interface that you want to view PPPoE client lease information.

Refresh—loads the latest PPPoE connection information from the security appliance for display.

interface connection

The *interface* connection node in the Monitoring > Interfaces tree only appears if static route tracking is configured. If you have several routes tracked, there will be a node for each interface that contains a tracked route.

See the following for more information about the route tracking information available:

- [Track Status for, page 41-9](#)
- [Monitoring Statistics for, page 41-9](#)

Track Status for

The Track Status for pane displays information about the the tracked object.

Fields

- Tracked Route—*Display only*. Displays the route associated with the tracking process.
- Route Statistics—*Display only*. Displays the reachability of the object, when the last change in reachability occurred, the operation return code, and the process that is performing the tracking.

Modes

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Monitoring Statistics for

The Monitoring Statics for pane displays statistics for the SLA monitoring process.

Fields

- SLA Monitor ID—*Display only*. Displays the ID of the SLA monitoring process.
- SLA statistics—*Display only*. Displays SLA monitoring statistics, such as the last time the process was modified, the number of operations attempted, the number of operations skipped, and so on.

Modes

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—



CHAPTER 42

Monitoring VPN

The VPN Monitoring sections show parameters and statistics for the following:

- VPN statistics for specific Remote Access, LAN-to-LAN, Clientless SSL VPN, and E-mail Proxy sessions
- Encryption statistics for tunnel groups
- Protocol statistics for tunnel groups
- Global IPSec and IKE statistics
- Crypto statistics for IPSec, IKE, SSL, and other protocols
- Statistics for cluster VPN server loads

VPN Connection Graphs

Displays VPN connection data in graphical or tabular form for the security appliance.

IPSec Tunnels

Use this window to specify graphs and tables of the IPSec tunnel types you want to view, or prepare to export or print.

Fields

- **Graph Window Title**—Displays the default title that appears in the window when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that window before printing or exporting it. To change the title, select an alternative from the drop-down list or type the title.
- **Available Graphs**—Shows the types of active tunnels you can view. For each type you want to view collectively in a single window, click the entry in this box and click Add.
- **Selected Graphs**—Shows the types of tunnels selected.

If you click Show Graphs, ASDM shows the active tunnels types listed in this box in a single window.

A highlighted entry indicates the type of tunnel to be removed from the list if you click Remove.

- **Add**—Moves the selected tunnel type from the Available Graphs box to the Selected Graphs box.

- **Remove**—Moves the selected tunnel type from the Selected Graphs box to the Available Graphs box.
- **Show Graphs**—Displays a window consisting of graphs of the tunnel types displayed in the Selected Graphs box. Each type in the window displayed has a Graph tab and a Table tab you can click to alternate the representation of active tunnel data.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Sessions

Use this panel to specify graphs and tables of the VPN session types you want to view, or prepare to export or print.

Fields

- **Graph Window Title**—Displays the default title that appears in the window when you click Show Graphs. This attribute is particularly useful when you want to clarify data in that window before printing or exporting it. To change the title, select an alternative from the drop-down list or type the title.
- **Available Graphs**—Shows the types of active sessions you can view. For each type you want to view collectively in a single window, click the entry in this box and click Add.
- **Selected Graphs**—Shows the types of active sessions selected.

If you click Show Graphs, ASDM shows all of the active session types listed in this box in a single window.

A highlighted entry indicates the type of session to be removed from the list if you click Remove.

- **Add**—Moves the selected session type from the Available Graphs box to the Selected Graphs box.
- **Remove**—Moves the selected session type from the Selected Graphs box to the Available Graphs box.
- **Show Graphs**—Displays a window consisting of graphs of the session types displayed in the Selected Graphs box. Each type in the window displayed has a Graph tab and a Table tab you can click to alternate the representation of active session data.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

VPN Statistics

These panels show detailed parameters and statistics for a specific remote-access, LAN-to-LAN, Clientless SSL VPN, or E-mail Proxy session. The parameters and statistics differ depending on the session protocol. The contents of the statistical tables depend on the type of connection you select. The detail tables show all the relevant parameters for each session.

Sessions

Use this panel to view session statistics for this server.

Fields

- Session types (unlabeled)—Lists the number of currently active sessions of each type, the total limit, and the total cumulative session count.
 - Remote Access—Shows the number of remote access sessions.
 - Site-to-Site—Shows the number of LAN-to-LAN sessions.
 - SSL VPN–Clientless—Shows the number of clientless browser-based VPN sessions.
 - SSL VPN–With Client—Shows the number of SSL VPN sessions requiring a client application on the remote computer.
 - SSL VPN–Total—Shows the number of client-based and clientless SSL VPN sessions.
 - E-mail Proxy—Shows the number of E-mail proxy sessions.
 - VPN Load Balancing—Shows the number of load-balanced VPN sessions
 - Total—Shows the total number of active concurrent sessions.
 - Total Cumulative—Shows the cumulative number of sessions since the last time the security appliance was rebooted or reset.
- Filter By—Specifies the type of sessions that the statistics in the following table represent.
 - Session type (unlabeled)—Designates the session type that you want to monitor. The default is Remote Access.
 - Session filter (unlabeled)—Designates which of the column heads in the following table to filter on. The default is --All Sessions--.
 - Filter name (unlabeled)—Specifies the name of the filter to apply. If you specify --All Sessions-- as the session filter list, this field is not available. For all other session filter selections, this field cannot be blank.
 - Filter—Executes the filtering operation.

The contents of the second table, also unlabeled, on this panel depend on the selection in the Filter By list. In the following list, the first-level bullets show the Filter By selection, and the second-level bullets show the column headings for this table.

- Remote Access—Indicates that the values in this table relate to remote access traffic.
 - Username/Tunnel Group—Shows the username or login name and the 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.
 - 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.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
 - NAC Result and Posture Token—Displays values in this column only if you configured Network Admission Control on the security appliance.

The NAC Result shows one of the following values:

Accepted—ACS successfully validated the posture of the remote host.

Rejected—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 security appliance.

Non-Responsive—The remote host did not respond to the EAPoUDP Hello message.

Hold-off—The security appliance 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 that is configurable on the Access Control Server. ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. The typical value of the Posture Token field that follows the NAC Result field is as follows: Healthy, Checkup, Quarantine, Infected, or Unknown.

- Site-toSite—Indicates that the values in this table relate to LAN-to-LAN traffic.
 - Tunnel Group/IP Address—Shows the name of the tunnel group and the IP address of the peer.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.

- Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
- Clientless SSL VPN—Indicates that the values in this table relate to Clientless SSL VPN traffic.
 - Username/IP Address—Shows the username or login name for the session and the IP address of the client.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.
- E-Mail Proxy—Indicates that the values in this table relate to traffic for Clientless SSL VPN sessions.
 - Username/IP Address—Shows the username or login name for the session and the IP address of the client.
 - Protocol/Encryption—Shows the protocol and the data encryption algorithm this session is using, if any.
 - Login Time/Duration—Shows the date and time (MMM DD HH:MM:SS) that the session logged in. and the length of the session. Time is displayed in 24-hour notation.
 - Client Type/Version—Shows the type and software version number (for example, rel. 7.0_int 50) for connected clients, sorted by username.
 - Bytes Tx/Bytes Rx—Shows the total number of bytes transmitted to/received from the remote peer or client by the security appliance.

The remainder of this section describes the buttons and fields beside and below the table.

- Details—Displays the details for the selected session. The parameters and values differ, depending on the type of session.
- Logout—Ends the selected session.
- Ping—Sends an ICMP `ping` (Packet Internet Groper) packet to test network connectivity. Specifically, the security appliance sends an ICMP Echo Request message to a selected host. If the host is reachable, it returns an Echo Reply message, and the security appliance 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 security appliance displays an Error screen with the name of the tested host.
- Logout By—Selects a criterion to use to filter the sessions to be logged out. If you select any but --All Sessions--, the box to the right of the Logout By list becomes active. If you selected the value Protocol for Logout By, the box becomes a list, from which you can select 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 box.
- Logout Sessions—Ends all sessions that meet the specified Logout By criteria.
- Refresh—Updates the screen and its data. The date and time indicate when the screen was last updated.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Sessions Details

The Session Details window displays configuration settings, statistics, and state information about the selected session.

The Remote Detailed table at the top of the Session Details window displays the following columns:

- **Username**—Shows the username or login name associated with the session. If the remote peer is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.
- **Group Policy and Tunnel Group**—Group policy assigned to the session and the name of the tunnel group upon which the session is established.
- **Assigned IP Address and Public IP Address**—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.
- **Protocol/Encryption**—Protocol and the data encryption algorithm this session is using, if any.
- **Login Time and Duration**—Time and date of the session initialization, and the length of the session. The session initialization time is in 24-hour notation.
- **Client Type and Version**—Type and software version number (for example, rel. 7.0_int 50) of the client on the remote computer.
- **Bytes Tx and Bytes Rx**—Shows the total number of bytes transmitted to and received from the remote peer by the security appliance.
- **NAC Result and Posture Token**—The ASDM displays values in this column only if you configured Network Admission Control on the security appliance.

The NAC Result shows one of the following values:

- **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 security appliance.
- **Non-Responsive**—The remote host did not respond to the EAPoUDP Hello message.
- **Hold-off**—The security appliance 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 security appliance 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 window displays the following columns:

- ID—Unique ID dynamically assigned to the session. The ID serves as the security appliance 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 an IKE session:

The following attributes apply to an IPSec session:

The following attributes apply to a NAC session:

- 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 security appliance 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 security appliance 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 security appliance. The Redirect URL is an optional part of the access policy payload. The security appliance 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 security appliance 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Sub-session Details – NAC Details

The NAC Details window lets you view the statistics and state of a NAC session, and revalidate and initialize the session or tunnel group.

The statistics and state attributes in this window are as follows:

- Reval Int (T)—Revalidation Time Interval. Interval in seconds required between each successful posture validation.
- Reval Left (T)—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.
- SQ Int (T)—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 security appliance to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
- EoU Age (T)—EAPoUDP Session Age. Number of seconds since the last successful posture validation.
- Hold Left (T)—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 security appliance 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 security appliance. The Redirect URL is an optional part of the access policy payload. The security appliance 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 security appliance 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.

The buttons in this window are as follows:



Note

Choose **Monitoring > VPN > VPN Statistics > NAC Session Summary** if you want to revalidate or initialize all sessions that are subject to posture validation.

- **Revalidate Session**—Click if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. Clicking this button initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you clicked this button remain in effect until the new posture validation succeeds or fails. Clicking this button does not affect the session if it is exempt from posture validation.
- **Initialize Session**—Click if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed, and you want to clear the resources assigned to the session. Clicking the button purges the EAPoUDP association and access policy, and initiates a new, unconditional posture validation. The NAC default ACL is effective during the revalidation, so the session initialization can disrupt user traffic. Clicking this button does not affect the session if it is exempt from posture validation.
- **Revalidate Tunnel Group**—Click if the posture of the peers in the tunnel group occupied by the selected session or the assigned access policies (that is, the downloaded ACLs), have changed. Clicking this button initiates new, unconditional posture validations. The posture validation and assigned access policy that were in effect for each session in the tunnel group 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 Tunnel Group**—Click if the posture of the peers in the tunnel group occupied by the selected session, 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 access policies (that is, the downloaded ACLs, if any) used for posture validation in the tunnel group occupied by the selected session, and initiates new, unconditional posture validations for the effected peers. 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Encryption Statistics

This panel shows the data encryption algorithms used by currently active user and administrator sessions on the security appliance. Each row in the table represents one encryption algorithm type.

Fields

- **Show Statistics For**—Selects a specific server or group or all tunnel groups.

- **Encryption Statistics**—Shows the statistics for all the data encryption algorithms in use by currently active sessions.
 - **Encryption Algorithm**—Lists the encryption algorithm to which the statistics in this row apply.
 - **Sessions**—Lists the number of sessions using this algorithm.
 - **Percentage**—Indicates the percentage of sessions using this algorithm relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).
- **Total Active Sessions**—Shows the number of currently active sessions.
- **Cumulative Sessions**—Shows the total number of sessions since the security appliance was last booted or reset.
- **Refresh**—Updates the statistics shown in the Encryption Statistics table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

NAC Session Summary

Monitoring > VPN > VPN Statistics > NAC Session Summary

The NAC Session Summary window lets you view the active and cumulative Network Admission Control sessions.

Fields

- **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 security appliance.
- **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 security appliance configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the security appliance for these peers. Otherwise, the security appliance assigns the NAC default policy.
- **Hold-off**—Number of peers for which the security appliance 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 security appliance. 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 security appliance, 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.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Protocol Statistics

This panel displays the protocols used by currently active user and administrator sessions on the security appliance. Each row in the table represents one protocol type.

Fields

- Show Statistics For—Selects a specific server or group or all tunnel groups.
- Protocol Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Protocol—Lists the protocol to which the statistics in this row apply.
 - Sessions—Lists the number of sessions using this protocol.
 - Percentage—Indicates the percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).
- Total Active Sessions—Shows the number of currently active sessions.
- Cumulative Sessions—Shows the total number of sessions since the security appliance was last booted or reset.
- Refresh—Updates the statistics shown in the Protocol Statistics table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

VLAN Mapping Sessions

This panel displays 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 security appliance forwards all traffic to the specified VLAN.

Field

- Active VLAN Mapping Sessions—Number of VPN sessions assigned to an egress VLAN.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Global IKE/IPSec Statistics

This panel displays the global IKE/IPSec statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one global statistic.

Fields

- Show Statistics For—Selects a specific protocol, IKE Protocol (the default) or IPSec Protocol.
- Global IKE/IPSec Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Global IKE/IPSec Statistics table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Crypto Statistics

This panel displays the crypto statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one crypto statistic.

Fields

- Show Statistics For—Selects a specific protocol, IKE Protocol (the default), IPSec Protocol, SSL Protocol, or other protocols.
- Crypto Statistics—Shows the statistics for all the protocols in use by currently active sessions.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Crypto Statistics table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Compression Statistics

This panel displays the compression statistics for currently active user and administrator sessions on the security appliance. Each row in the table represents one compression statistic.

Fields

- Show Statistics For—Lets you select compression statistics for clientless SSL VPN or SSL VPN Client sessions.
- Statistics—Shows all the statistics for the selected VPN type.
 - Statistic—Lists the name of the statistical variable. The contents of this column vary, depending upon the value you select for the Show Statistics For parameter.
 - Value—The numerical value for the statistic in this row.
- Refresh—Updates the statistics shown in the Compression Statistics table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Cluster Loads

Use this panel to view 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.

Fields

- **VPN Cluster Loads**—Displays the current load distribution in the VPN load-balancing cluster. Clicking a column heading sorts the table, using the selected column as the sort key.
 - **Public IP Address**—Displays the externally visible IP address for the server.
 - **Role**—Indicates whether this server is a master or backup device in the cluster.
 - **Priority**—Shows the priority assigned to this server in the cluster. The priority must be an integer in the range of 1 (lowest) to 10 (highest). The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster.
 - **Model**—Indicates the security appliance model name and number for this server.
 - **Load %**—Indicates what percentage of a server's total capacity is in use, based upon the capacity of that server.
 - **Sessions**—Shows the number of currently active sessions.
- **Refresh**—Loads the table with updated statistics.

Modes

The following table shows the modes in which this feature is available:

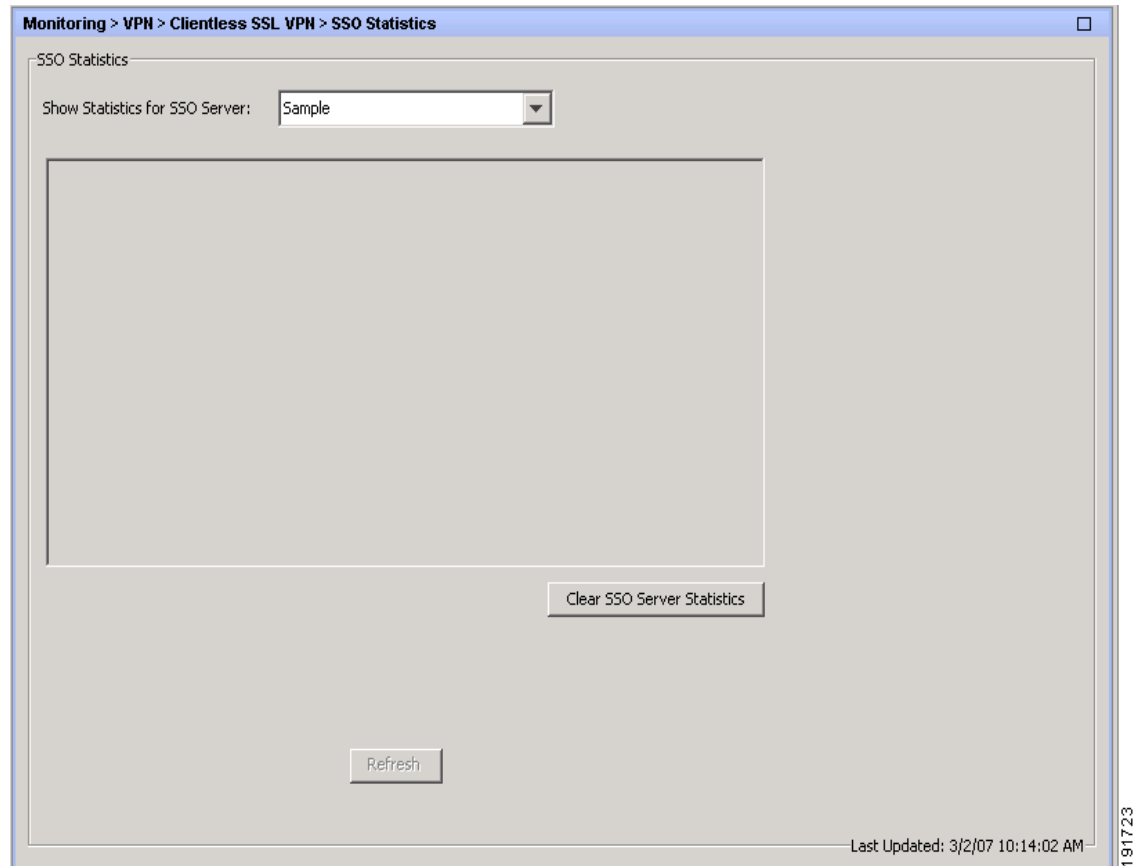
Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SSO Statistics for Clientless SSL VPN Session

This panel displays the single sign-on statistics for currently active SSO servers configured for the security appliance.

**Note**

These statistics are for SSO with SiteMinder and SAML Browser Post Profile servers only.

**Fields**

- Show Statistics For SSO Server — Selects an SSO server.
- SSO Statistics—Shows the statistics for all the currently active sessions on the selected SSO server.
SSO statistics that display include:
 - Name of SSO server
 - Type of SSO server
 - Authentication Scheme Version (SiteMinder servers)
 - Web Agent URL (SiteMinder servers)
 - Assertion Consumer URL (SAML POST servers)
 - Issuer (SAML POST servers)
 - Number of pending requests
 - Number of authorization requests
 - Number of retransmissions
 - Number of accepts

- Number of rejects
 - Number of timeouts
 - Number of unrecognized responses
- Refresh—Updates the statistics shown in the SSO Statistics table
- Clear SSO Server Statistics—Resets statistics for the displayed server.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—



CHAPTER 43

Monitoring Routing

You can use ASDM to monitor OSPF LSAs, OSPF and EIGRP neighbors, and the routing table. To access the routing monitoring screens, go to **Monitoring > Routing** in the ASDM interface.

This section contains the following topics:

- [Monitoring OSPF LSAs, page 43-1](#)
- [Monitoring OSPF Neighbors, page 43-5](#)
- [Monitoring EIGRP Neighbors, page 43-7](#)
- [Displaying Routes, page 43-8](#)

Monitoring OSPF LSAs

You can view the LSAs stored in the security appliance OSPF database in the **Monitoring > Routing > OSPF LSAs** area. There are 4 types of LSAs stored in the database, each with its own particular format. The following briefly describes the LSA types:

- Router LSAs (Type 1 LSAs) describe the routers attached to a network.
- Network LSAs (Type 2 LSAs) describe the networks attached to an OSPF router.
- Summary LSAs (Type 3 and Type 4 LSAs) condense routing information at area borders.
- External LSAs (Type 5 and Type 7 LSAs) describe routes to external networks.

To learn more about the information displayed for each LSAs type, see the following:

- [Type 1](#)
- [Type 2](#)
- [Type 3](#)
- [Type 4](#)
- [Type 5](#)
- [Type 7](#)

Type 1

Type 1 LSAs are router link advertisements that are passed within an area by all OSPF routers. They describe the router links to the network. Type 1 LSAs are only flooded within a particular area.

The Type 1 pane displays all Type 1 LSAs received by the security appliance. Each row in the table represents a single LSA.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Router ID—*Display only*. Displays the OSPF router ID of the router originating the LSA.
- Advertiser—*Display only*. Displays the ID of the router originating the LSA. For router LSAs, this is identical to the Router ID.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.
- Link Count—*Display only*. Displays the number of interfaces detected for the router.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Type 2

Type 2 LSAs are network link advertisements that are flooded within an area by the Designated Router. They describe the routers attached to specific networks.

The Type 2 pane displays the IP address of the Designated Router that advertises the routes.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Designated Router—*Display only*. Displays the IP address of the Designated Router interface that sent the LSA.
- Advertiser—*Display only*. Displays the OSPF router ID of the Designated Router that sent the LSA.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Type 3

Type 3 LSA are summary link advertisements that are passed between areas. They describe the networks within an area.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Destination—*Display only*. Displays the address of the destination network being advertised.
- Advertiser—*Display only*. Displays the ID of the ABR that sent the LSA.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Type 4

Type 4 LSAs are summary link advertisements that are passed between areas. They describe the path to the ASBR. Type 4 LSAs do not get flooded into stub areas.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Router ID—*Display only*. Displays the router ID of the ASBR.
- Advertiser—*Display only*. Displays the ID of the ABR that sent the LSA.
- Age—*Display only*. Displays the age of the link state.

- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Type 5

Type 5 LSAs are passed between and flooded into areas by ASBRs. They describe routes external to the AS. Stub areas and NSSAs do not receive these LSAs.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Network—*Display only*. Displays the address of the AS external network.
- Advertiser—*Display only*. Displays the router ID of the ASBR.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.
- Tag—*Display only*. Displays the external route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Type 7

Type 7 LSAs are NSSA AS-external routes that are flooded by the ASBR. They are similar to Type 5 LSAs, but unlike Type 5 LSAs, which are flooded into multiple areas, Type 7 LSAs are only flooded into NSSAs. Type 7 LSAs are converted to Type 5 LSAs by ABRs before being flooded into the area backbone.

Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Network—*Display only*. Displays the address of the external network.
- Advertiser—*Display only*. Displays the router ID of the ASBR that sent the LSA.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.
- Tag—*Display only*. Displays the external route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Monitoring OSPF Neighbors

The OSPF Neighbor pane displays the OSPF neighbors dynamically discovered and statically configured OSPF neighbors on the security appliance. The OSPF Neighbor pane is located at **Monitoring > Routing > OSPF Neighbors** in the ASDM interface.

Fields

- Neighbor—*Display only*. Displays the neighbor router ID.
- Priority—*Display only*. Displays the router priority.
- State—*Display only*. Displays the OSPF state for the neighbor:
 - Down—This is the first OSPF neighbor state. It means that no hello packets have been received from this neighbor, but hello packets can still be sent to the neighbor in this state.
During the fully adjacent neighbor state, if the security appliance does not receive hello packet from a neighbor within the dead interval time, or if the manually configured neighbor is being removed from the configuration, then the neighbor state changes from Full to Down.
 - Attempt—This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the security appliance sends unicast hello packets every poll interval to the neighbor from which hellos have not been received within the dead interval.
 - Init—This state specifies that the security appliance has received a hello packet from its neighbor, but the ID of the receiving router was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the router ID of the sender in its hello packet as an acknowledgment that it received a valid hello packet.

- **2-Way**—This state designates that bi-directional communication has been established between the security appliance and the neighbor. Bi-directional means that each device has seen the hello packet from the other device. This state is attained when the router receiving the hello packet sees its own Router ID within the neighbor field of the received hello packet. At this state, the security appliance decides whether to become adjacent with this neighbor. On broadcast media and non-broadcast multiaccess networks, a the security appliance becomes full only with the designated router and the backup designated router; it stays in the 2-way state with all other neighbors. On point-to-point and point-to-multipoint networks, the security appliance becomes full with all connected neighbors.

At the end of this stage, the DR and BDR for broadcast and non-broadcast multiaccess networks are elected.

**Note**

Receiving a Database Descriptor packet from a neighbor in the Init state will also cause a transition to 2-way state.

- **Exstart**—Once the DR and BDR are elected, the actual process of exchanging link state information begins between the security appliance and the DR and BDR.

In this state, the security appliance and the DR and BDR establish a master-slave relationship and choose the initial sequence number for adjacency formation. The device with the higher router ID becomes the master and starts the exchange and is therefore the only device that can increment the sequence number.

**Note**

DR/BDR election occurs by virtue of a higher priority configured on the device instead of highest router ID. Therefore, it is possible that a DR plays the role of slave in this state. Master/slave election is on a per-neighbor basis. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR.

- **Exchange**—In the exchange state, OSPF neighbors exchange DBD packets. Database descriptors contain LSA headers only and describe the contents of the entire link state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link state request packets and link state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link state database to check if new or more current link state information is available with the neighbor.
- **Loading**—In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link state request packets. The neighbor then provides the requested link state information in link state update packets. During the adjacency, if a the security appliance receives an outdated or missing LSA, it requests that LSA by sending a link state request packet. All link state update packets are acknowledged.
- **Full**—In this state, the neighbors are fully adjacent with each other. All the router and network LSAs are exchanged and the router databases are fully synchronized.
Full is the normal state for an OSPF router. The only exception to this is the 2-way state, which is normal in a broadcast network. Routers achieve the full state with their DR and BDR only. Neighbors always see each other as 2-way.
- **Dead Time**—*Display only*. Displays the amount of time remaining that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.
- **Address**—*Display only*. Displays the IP address of the interface to which this neighbor is directly connected.

- Interface—*Display only*. Displays the interface on which the OSPF neighbor has formed adjacency.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Monitoring EIGRP Neighbors

The EIGRP Neighbors pane displays dynamically discovered EIGRP neighbors. Statically defined neighbors do not appear in this pane. To see the statically defined EIGRP neighbors, see **Configuration > Device Setup > Routing > EIGRP > Static Neighbor**.

Fields

- Address—IP address of the EIGRP neighbor.
- Interface—Interface on which the security appliance receives hello packets from the neighbor.
- Holdtime—Length of time (in seconds) that the security appliance waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor.

If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed.

If this value reaches 0, the security appliance considers the neighbor unreachable.

- Uptime—Elapsed time (in hours:minutes: seconds) since the security appliance first heard from this neighbor.
- Queue Length—Number of EIGRP packets (update, query, and reply) that the security appliance is waiting to send.
- Sequence Number—Sequence number of the last update, query, or reply packet that was received from the neighbor.
- SRTT—Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the security appliance to receive an acknowledgment of that packet.
- RTO—Retransmission timeout (in milliseconds). This is the amount of time the security appliance waits before resending a packet from the retransmission queue to a neighbor.
- Clear Neighbors—Click the Clear Neighbors button to clear dynamically-learned neighbors from the neighbor table.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Displaying Routes

The Routes pane displays the statically configured, connected, and discovered routes in the security appliance routing table.

Fields

- Protocol—*Display only*. Displays the origin of the route information.
 - RIP—The route was derived using RIP.
 - OSPF—The route was derived using OSPF.
 - EIGRP—The route was derived using EIGRP.
 - CONNECTED—The route is a network directly connected to the interface.
 - STATIC—The route is statically defined.
- Type—*Display only*. Displays the type of route. It can be one of the following values:
 - (dash)—Indicates that the type column does not apply to the specified route.
 - IA—The route is an OSPF interarea route.
 - E1—The route is an OSPF external type 1 route.
 - E2—The route is an OSPF external type 2 route.
 - N1—The route is an OSPF not so stubby area (NSSA) external type 1 route.
 - N2—The route is an OSPF NSSA external type 2 route.
- Destination—*Display only*. Displays the IP address/netmask of the destination network.
- Gateway—*Display only*. Displays the IP address of the next router to the remote network.
- Interface—*Display only*. Displays the interface through which the specified network can be reached.
- [AD/Metric]—*Display only*. Displays the administrative distance/metric for the route.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—



CHAPTER 44

Monitoring Properties

This chapter includes the following sections:

- [Monitoring AAA Servers, page 44-1](#)
- [Monitoring Device Access, page 44-4](#)
- [Connection Graphs](#)
- [CRL](#)
- [DNS Cache](#)
- [IP Audit](#)
- [System Resources Graphs](#)
- [WCCP](#)

Monitoring AAA Servers

This section includes the following topics:

- [Viewing AAA Server Statistics, page 44-1](#)
- [Updating the Operational State of an AAA Server, page 44-2](#)
- [Fields Used to Monitor AAA Servers, page 44-3](#)

Viewing AAA Server Statistics

Use this procedure to view statistics for AAA Servers.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM Startup Wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).

Procedure

To view AAA Server statistics, perform the following steps.

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click **AAA Servers**.
The AAA Servers dialog box opens in the right-hand pane, displaying a list of the configured AAA servers.
- Step 4** Click the row for the server whose statistics you want to monitor.
Statistics for the selected server display in the lower portion of the dialog box.
-

Updating the Operational State of an AAA Server

Use this procedure to update the operational state of an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM Startup Wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).

Procedure

To update the state of an AAA Server, perform the following steps.

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click **AAA Servers**.
The AAA Servers dialog box opens in the right-hand pane, displaying a list of the AAA servers that are configured on the security appliance.
- Step 4** Click the row for the server to update.
Statistics for the selected server display in the lower portion of the dialog box.
- Step 5** Click **Update Server Statistics**.
The Update Server Statistics dialog box opens.
- Step 6** From the AAA Server Status selection list, choose the operational state to apply to this server.
The security appliance is updated with the server current state.
- Step 7** Click **OK**.

The dialog box closes.

Fields Used to Monitor AAA Servers

The following table describes the fields for monitoring AAA Servers.

Field	Description
Server Group	The name of the server group where the server resides.
Protocol	The protocol used by the AAA server group.
IP Address	The IP address for the AAA server.
Status	The operational status of the AAA server. <ul style="list-style-type: none">• Active• Failed
Statistics	The lower portion of the AAA Servers dialog box shows the following current information about the selected server: <ul style="list-style-type: none">• Server port and/or hostname• Number of pending requests• Average round trip time• Number of authentication requests• Number of authorization requests• Number of accounting requests• Number of retransmissions• Number of accepts• Number of rejects• Number of challenges• Number of malformed responses• Number of bad authenticators• Number of timeouts• Number of unrecognized responses
Clear Server Statistics	Zeroes the counters for the selected server's statistics.
Update Server Status	Opens the Update Server Status dialog box for changing the operational state of the AAA server.
Refresh	Refreshes the dialog box display.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Monitoring Device Access

This section includes the following topics:

- [Monitoring User Lockouts](#)
- [Monitoring Authenticated Users](#)
- [Monitoring Active Sessions](#)
- [Fields Used to Monitor Device Access](#)

Monitoring User Lockouts

This section includes the following topics:

- [Viewing Lockouts, page 44-5](#)
- [Removing All User Lockouts, page 44-6](#)
- [Removing One User Lockout, page 44-7](#)

Viewing Lockouts

Use this procedure to view information about users who were locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To view information about user lockouts, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.

The monitoring functions display in the left-hand Navigation pane.

Step 2 Click **Properties**.

The Properties Navigation pane opens.

Step 3 Click the plus (+) symbol next to Device Access.

The list of Device Access functions expands below it.

Step 4 Click **AAA Local Locked Out Users**.

The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server.

Removing All User Lockouts

Use this procedure to remove the lockouts of all users who were locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To clear all user lockouts from the security appliance, perform the following steps:

Step 1 From the ASDM toolbar, click **Monitoring**.

The monitoring functions display in the left-hand Navigation pane.

Step 2 Click **Properties**.

The Properties Navigation pane opens.

Step 3 Click the plus (+) symbol next to Device Access.

The list of Device Access functions expands below it.

Step 4 Click **AAA Local Locked Out Users**.

The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server.

Step 5 Click **Refresh**.

The display is refreshed with current lockout information.

Step 6 Review the refreshed list to make sure that you want to remove all lockouts.**Step 7** Click **Clear All Lockouts**.

All lockouts from the security appliance are removed and usernames removed from the list.

Removing One User Lockout

Use this procedure to remove a lockout for one user who was locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To remove a user lockout, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | From the ASDM toolbar, click Monitoring .
The monitoring functions display in the left-hand Navigation pane. |
| Step 2 | Click Properties .
The Properties Navigation pane opens. |
| Step 3 | Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it. |
| Step 4 | Click AAA Local Locked Out Users .
The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server. |
| Step 5 | Select the username from the list.
The row is highlighted. |
| Step 6 | Click Clear Selected Lockout .
The lockout is removed for this user and the row is removed from the list. |
-

Monitoring Authenticated Users

Use this procedure to monitor users who have successfully authenticated with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To monitor information about users who have successfully authenticated, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | From the ASDM toolbar, click Monitoring .

The monitoring functions display in the left-hand Navigation pane. |
| Step 2 | Click Properties .

The Properties Navigation pane opens. |
| Step 3 | Click the plus (+) symbol next to Device Access.

The list of Device Access functions expands below it. |
| Step 4 | Click Authenticated Users .

The Authenticated Users dialog box opens in the right-hand pane, displaying a list of users who have successfully authenticated with an AAA server. |
-

Monitoring Active Sessions

This section includes the following procedures:

- [Viewing Active Sessions, page 44-9](#)
- [Disconnecting an Active Session, page 44-11](#)

Viewing Active Sessions

Use this procedure to view the sessions that are currently connected to the security appliance.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).

- You have already configured the security appliance access for the session traffic you want to monitor. See the procedures in one of the following sections:
 - [Configuring Device Access, page 16-1](#)
 - [Configuring CLI Parameters, page 16-2](#)

Procedure

To monitor active sessions, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **ASDM/HTTPS/Telnet/SSH Sessions**.
A dialog box opens in the right-hand pane, displaying the list of currently active connections.
The following table describes the fields for monitoring active ASDM/HTTPS/Telnet sessions.

Field	Description
Type	The type of connection (ASDM/HTTPS/Telnet).
Session ID	The name of a currently connected ASDM/HTTPS/Telnet session.
IP Address	The IP address of the host or network that is currently connected to the security appliance.
Disconnect	Disconnects the selected ASDM/HTTPS/Telnet session from the security appliance.
Refresh	Refreshes the dialog box display.

The following table describes the fields for monitoring active SSH sessions.

Field	Description
Client	The client type for the selected SSH session.
User	The user name for the selected SSH session.
State	The state of the selected SSH session.
Version	The version of SSH used to connect to the security appliance.
Encryption (In)	The inbound encryption method used for the selected session.
Encryption (Out)	The outbound encryption method used for the selected session.
HMAC (In)	The configured HMAC for the selected inbound SSH session.
HMAC (Out)	The configured HMAC for the selected outbound SSH session.
SID	The session ID of the selected session.
Disconnect	Disconnects an active SSH session connected to the security appliance.
Refresh	Refreshes the dialog box display.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Disconnecting an Active Session

Use this procedure to disconnect an active ASDM/HTTPS, SSH, or Telnet session that is currently connected to the security appliance.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-17](#).
- You have already configured the security appliance access. See the procedures in one of the following sections:
 - [Configuring Device Access, page 16-1](#)
 - [Configuring CLI Parameters, page 16-2](#)

Procedure

To disconnect an active security appliance session, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **ASDM/HTTPS/Telnet/SSH Sessions**.
A dialog box opens in the right-hand pane, displaying a table which lists the currently active connections.
- Step 5** In the table, select the session you want to disconnect.
The row is highlighted.
- Step 6** Click **Disconnect**.
The session is disconnected from the security appliance, and removed from the table.
-

Fields Used to Monitor Device Access

This section includes the following topics:

- [Fields for Monitoring User Lockouts, page 44-12](#)
- [Fields for Monitoring Users Who Have Authenticated with a Server, page 44-13](#)

Fields for Monitoring User Lockouts

The following table describes the fields for monitoring locked out users.

Field	Description
Lock Time	The amount of time that the user has been locked out of the system.
Failed Attempts	The number of authentication attempts that the user failed.
User	A list of usernames of those users who are currently locked out of the security appliance because they were unable to successfully authenticate with the authentication server.
Clear Selected Lockout	Removes the lockout for the selected username and removes the username from the list.
Clear All Lockouts	Removes the lockout for all usernames in the list. Note We recommend that you refresh the list of locked out users and review it before clearing all lockouts.
Refresh	Refreshes the dialog box display.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Fields for Monitoring Users Who Have Authenticated with a Server

The following table describes the fields for monitoring authenticated users.

Field	Description
User	The usernames of users who have successfully authenticated with an authentication server.
IP Address	The IP addresses of users who have successfully authenticated with an authentication server.
Dynamic ACL	The dynamic access list of the user authenticated to use the security appliance.
Inactivity Timeout	The amount of time that the user connection must remain inactive before the session times out and the user is disconnected.
Absolute Timeout	The amount of time that the user can remain connected before the session closes and the user is disconnected.
Refresh	Refreshes the dialog box display.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Connection Graphs

The Connection Graphs pane lets you view connection information about the security appliance in graph format. You can view information about NAT and performance monitoring information, including UDP connections, AAA performance, and inspection information. This section includes the following topics:

- [Perfmon](#)
- [Xlates](#)

Perfmon

The Perfmon pane lets you view the performance information in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - AAA Perfmon—Displays the security appliance AAA performance information.
 - Inspection Perfmon—Displays the security appliance inspection performance information.
 - Web Perfmon—Displays the security appliance web performance information, including URL access and URL server requests.
 - Connections Perfmon—Displays the security appliance connections performance information.
 - Xlate Perfmon—Displays the security appliance NAT performance information.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Xlates

This pane lets you view the active Network Address Translations in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - Xlate Utilization—Displays the security appliance NAT utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected entry from the Selected Graphs list.

- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CRL

This pane allows you to view or clear associated CRLs of selected CA certificates.

Fields

- CA Certificate Name—Choose the name of the selected certificate from the drop-down list.
- View CRL—Click to view the selected CRL.
- Clear CRL—Click to clear the selected CRL from the cache.
- CRL Info—*Display only*. Displays detailed CRL information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DNS Cache

The security appliance provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache along with its corresponding hostname.

Important Notes

- DNS cache entries are time stamped. The time stamp will be used to age out unused entries. When the entry is added to the cache, the time stamp is initialized. Each time the entry is accessed, the timestamp is updated. At a configured time interval, the DNS cache will check all entries and purge those entries whose time exceeds a configured age-out timer.

- If new entries arrive but there is no room in the cache because the size was exceeded or no more memory is available, the cache will be thinned by one third, based on the entries age. The oldest entries will be removed.

Fields

- Host—Shows the DNS name of the host.
- IP Address—Shows the address that resolves to the hostname.
- Permanent—Indicates whether the entry was made though a **name** command.
- Idle Time—Specifies the time elapsed since the security appliance last referred to that entry.
- Active—Indicates whether the entry has aged out. If there is not adequate space in cache, this entry may be deleted.
- Clear Cache—Click to clear the entire DNS cache.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

IP Audit

The IP Audit pane lets you view the number of packets that match informational and attack signatures that are shown in graphical or tabular form. Each graph type shows the combined packets for all interfaces that have this feature enabled.

Fields

- Available Graphs—Lists the types of signatures available for monitoring. See [IP Audit Signatures](#) for detailed information about each signature type. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.
 - IP Options—Shows the packet count for the following signatures:
 - Bad Options List (1000)
 - Timestamp (1002)
 - Provide s, c, h, tcc (1003)
 - SATNET ID (1005)
 - IP Route Options—Shows the packet count for the following signatures:
 - Loose Source Route (1004)
 - Record Packet Route (1001)
 - Strict Source Route (1006)
 - IP Attacks—Shows the packet count for the following signatures:
 - IP Fragment Attack (1100)

- Impossible IP Packet (1102)
- IP Teardrop (1103)
- ICMP Requests—Shows the packet count for the following signatures:
 - Echo Request (2004)
 - Time Request (2007)
 - Info Request (2009)
 - Address Mask Request (2011)
- ICMP Responses—Shows the packet count for the following signatures:
 - Echo Reply (2000)
 - Source Quench (2002)
 - Redirect (2003)
 - Time Exceeded (2005)
 - Parameter Problem (2006)
- ICMP Replies—Shows the packet count for the following signatures:
 - Unreachable (2001)
 - Time Reply (2008)
 - Info Reply (2010)
 - Address Mask reply (2012)
- ICMP Attacks—Shows the packet count for the following signatures:
 - Fragmented ICMP (2150)
 - Large ICMP (2151)
 - Ping of Death (2154)
- TCP Attacks—Shows the packet count for the following signatures:
 - No Flags (3040)
 - SYN & FIN Flags Only (3041)
 - FIN Flag Only (3042)
- UDP Attacks—Shows the packet count for the following signatures:
 - Bomb (4050)
 - Snork (4051)
 - Chargen (4052)
- DNS Attacks—Shows the packet count for the following signatures:
 - Host Info (6050)
 - Zone Transfer (6051)
 - Zone Transfer High Port (6052)
 - All Records (6053)
- FTP Attacks—Shows the packet count for the following signatures:
 - Improper Address (3153)
 - Improper Port (3154)

- RPC Requests to Target Hosts—Shows the packet count for the following signatures:
 - Port Registration (6100)
 - Port Unregistration (6101)
 - Dump (6102)
- YP Daemon Portmap Requests—Shows the packet count for the following signatures:
 - ypserv Portmap Request (6150)
 - yplib Portmap Request (6151)
 - yppasswdd Portmap Request (6152)
 - ypupdated Portmap Request (6153)
 - ypxfrd Portmap Request (6154)
- Miscellaneous Portmap Requests—Shows the packet count for the following signatures:
 - mountd Portmap Request (6155)
 - rexed Portmap Request (6175)
- Miscellaneous RPC Calls—Shows the packet count for the following signatures:
 - rexed Attempt (6180)
- RPC Attacks—Shows the packet count for the following signatures:
 - statd Buffer Overflow (6190)
 - Proxied RPC (6103)
- Add—Click to add the selected graph type to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.
- Selected Graphs—Lists the graph types you want to show in the Selected Graphs list.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Resources Graphs

This pane lets you view the status of the security appliance memory, CPU, and block utilization. This section includes the following topics:

- [Blocks](#)
- [CPU](#)
- [Memory](#)

Blocks

This pane lets you view the free and used memory blocks. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - Blocks Used—Displays the security appliance used memory blocks.
 - Blocks Free—Displays the security appliance free memory blocks.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CPU

This pane lets you view the CPU utilization. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - CPU Utilization—Displays the security appliance CPU utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Memory

This pane lets you view the memory utilization. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - Free Memory—Displays the security appliance free memory.
 - Used Memory—Displays the security appliance used memory.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

WCCP

The Web Cache Communication Protocol redirects IPv4 traffic flows to web caches in real-time. In ASDM, you can monitor packet redirection of an interface using WCCP. WCCP also provides load balancing, scaling, fault tolerance, and fail safe services. Load balancing is provided by hashing based on the destination IP address. The hash values are used to choose the egress interface for any traffic flow.

This protocol also enables the security appliance and WCCP clients to form service groups to support a service. This section includes the following topics:

- [Service Groups](#)
- [Redirection](#)

Service Groups

This pane allows you to view and refresh the service group, the display mode, and hash settings, which include the source and destination IP addresses and the source and destination port numbers.

Fields

- Service Group—Choose the applicable service group from the drop-down list.
- Display Mode—Choose the display mode from the drop-down list.
- Destination IP Address—Specify the destination IP address.
- Source IP Address—Specify the source IP address.
- Destination Port—Specify the destination port number.
- Source Port—Specify the source port number.
- WCCP Service Groups—*Display-only*. Shows the selected WCCP service group information.

For example:

```
Global WCCP information:
  Router information:
    Router Identifier:          -not yet determined-
    Protocol Version:          2.0

    Service Identifier: web-cache
    Number of Cache Engines:    0
    Number of routers:          0
    Total Packets Redirected:    0
    Redirect access-list:       -none-
    Total Connections Denied Redirect: 0
    Total Packets Unassigned:    0
    Group access-list:          -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0

    Service Identifier: 1
    Number of Cache Engines:    0
    Number of routers:          0
    Total Packets Redirected:    0
    Redirect access-list:       -none-
    Total Connections Denied Redirect: 0
    Total Packets Unassigned:    0
    Group access-list:          -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0
```

Redirection

This pane allows you to view and refresh WCCP interface statistics in either a summary or detailed format.

Fields

- Show Summary—Choose this option to display statistics in a summary format.
- Show Details—Choose this option to display statistics in a detailed format.

- WCCP Interface Statistics—*Display-only*. Shows the current WCCP interface statistics.

For example:

WCCP interface configuration details:

```
Management0/0
Output services: 0
Input services: 1
Static:         None
Dynamic:        001
Mcast services: 0
Exclude In:     FALSE
```




CHAPTER 45

Monitoring Logging

You can view real-time syslog messages that appear in the log buffer. When you open the Cisco ASDM 6.1(3) for ASA 8.0(4) main application window, the most recent ASDM system log messages appear at the bottom of a scrolling window.

You can use these messages to help troubleshoot errors or monitor system usage and performance. For a description of the Logging feature, see [Chapter 17, “Configuring Logging.”](#)

About Log Viewing

This section describes syslog message viewing, and includes the following topics:

- [Log Buffer, page 45-1](#)
- [Real-Time Log Viewer, page 45-3](#)

Log Buffer

The Log Buffer pane lets you view syslog messages that have been saved in the buffer in a separate window. To access this pane, choose **Monitoring > Logging > Log Buffer**.

To view the log buffer, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Choose the level of logging messages to view, ranging from Emergency to Debugging, from the drop-down list. For more information about severity levels, see Chapter 17, “Configuring Logging.” |
| Step 2 | Click View to open a separate window in which log messages appear. To continue, see Log Buffer Viewer, page 45-2 . |
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Log Buffer Viewer

The Log Buffer Viewer pane lets you view messages that appear in the log buffer, an explanation of the message, details about the message, and recommended actions to take, if necessary, to resolve an error. To access this pane, choose **Monitoring > Logging > Log Buffer > View**.

To use the log buffer viewer, perform the following steps:

-
- Step 1** Right-click a message to display a menu from which you can select from the Refresh, Copy Selected Log Entry, Save Log, Clear Display, Color Settings, Create Access Rule, Show Access Rule, and Show Details options. A list of icons associated with each severity level appears at the bottom of this pane.
- Step 2** Choose from the following actions:
- Click **Refresh** to refresh the display.
 - Click **Copy Selected Log Entry** to copy a selected message.
 - Click **Save Log** to save the contents of the log to your computer.
 - Click **Clear Display** to clear the list of messages.
 - Click **Color Settings** to specify that messages of different severity levels display in different colors.
 - Click **Create Access Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
 - Click **Show Access Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to system log message IDs 106100 and 106023.
 - Click **Show Details** to show or hide the Explanation, Recommended Action, and Details tabs. The Explanation tab provides the message syntax, an explanation for the message, and the suggested corrective action to take, if any. The Recommended Action tab describes what you should do when you receive this message. The Details tab lists the date, time, severity level, syslog ID, source IP address, destination IP address, and a description of the message.
 - In the Find field, enter text that you want to find in messages, and click the **Search** icon to start the search.
 - Click **Help** to obtain more information.
 - Enter text to filter messages by in the Filter By drop-down list, then press **Enter** or click **Filter** to apply the filter to the displayed messages. Click **Show All** to display all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed syslog messages.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Real-Time Log Viewer

The Real-Time Log Viewer lets you view real-time syslog messages in a separate window. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer**.

To view syslog messages in real-time, perform the following steps:

-
- Step 1** Choose the level of logging messages to view, ranging from Emergency to Debugging, from the drop-down list.
- Step 2** Enter the buffer limit, which is the maximum number of syslog messages to view. The default is 1000.
- Step 3** Click **View** to open a separate window in which syslog messages appear. To continue, see [Real-Time Log Viewer, page 45-3](#).
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Real-Time Log Viewer

The Real-Time Log Viewer pane lets you view incoming messages in real-time and filter them based on text that you specify. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer > View**.

To use the real-time log viewer, perform the following steps:

-
- Step 1** Right-click a message in the viewer to display a menu from which you can select from the Pause, Copy Selected Log Entry, Save Log, Clear Display, Color Settings, Create Access Rule, Show Access Rule, and Show Details options. A list of color-coded icons that are associated with each severity level appears at the bottom of this pane. For more information about severity levels, see [Chapter 17, “Configuring Logging.”](#)
- Step 2** Choose from the following actions:
- Click **Pause** to stop the scrolling of the display.
 - Click **Copy Selected Log Entry** to copy a selected message.

- Click **Save Log** to save the contents of the log to your computer.
- Click **Clear Display** to clear the list of messages.
- Click **Color Settings** to specify that messages of different severity levels display in different colors.
- Click **Create Access Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- Click **Show Access Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to syslog message IDs 106100 and 106023.
- Click **Show Details** to show or hide the Explanation, Recommended Action, and Details tabs. The Explanation tab provides the message syntax, an explanation for the message, and the suggested corrective action to take, if any. The Recommended Action tab describes what you should do when you receive this message. The Details tab lists the date, time, severity level, syslog ID, source IP address, destination IP address, and a description of the message.
- In the Find field, enter text that you want to find in messages, and click the **Search** icon to start the search.
- Click **Help** to obtain more information.
- Enter text to filter messages by in the Filter By drop-down list, then press **Enter** or click **Filter** to apply the filter to the displayed messages. Click **Show All** to display all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed log messages.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—



CHAPTER 46

Monitoring Failover

Failover monitoring in ASDM depends upon the mode of the device. In single context mode, or within a security context in multiple context mode, you can monitor the state of failover for the device and view stateful failover statistics. In the system execution space of multiple context mode, you can monitor the failover state for each failover group

For more information about monitoring failover in each of these system configurations, see the following topics:

- [Monitoring Failover in Single Context Mode or in a Security Context, page 46-1](#)
- [Monitoring Failover in the System Execution Space, page 46-6](#)

Monitoring Failover in Single Context Mode or in a Security Context

You can monitor the status of the active and standby devices in a failover pair and failover related statistics in the **Monitoring > Properties > Failover** area. See the following screens for more information:

- [Status](#)—Displays the failover status of the device.
- [Graphs](#)—Displays graphs of various failover communication statistics.

For More Information

For more information about failover in general, see [Understanding Failover](#).

Status

The Status pane displays the failover state of the system. In single context mode, you can also control the failover state of the system by:

- Toggling the active/standby state of the device.
- Resetting a failed device.
- Reloading the standby unit.

In multiple context mode, you can control these settings in the system execution space. See [Monitoring Failover in the System Execution Space, page 46-6](#).

Fields

Failover state of the system—*Display only*. Displays the failover state of the security appliance. The information in this field is the same output you would receive from the show failover command. The following information is included in the display:



Note

Only a subset of the fields below appear when viewing the failover status within a security context. Those fields are indicated by an asterisk (*) before the field name.

- *Failover—Displays “On” when failover is enabled, “Off” when failover is not enabled.
- Cable Status—(PIX security appliance platform only) Displays the status of the serial failover cable. The following shows possible cable states:
 - Normal—The cable is connected to both units, and they both have power.
 - My side not connected—The serial cable is not connected to this unit. It is unknown if the cable is connected to the other unit.
 - Other side is not connected—The serial cable is connected to this unit, but not to the other unit.
 - Other side powered off—The other unit is turned off.
 - N/A—LAN-based failover is enabled.
- Failover unit—Displays the role of the system in the failover pair, either “Primary” or “Secondary”.
- Failover LAN Interface—Displays the logical and physical name of the LAN failover interface. If you are using the dedicated failover cable on the PIX platform, this field displays “N/A - Serial-based failover enabled”. If you have not yet configured the failover interface, this field displays “Not configured”.
- Unit Poll frequency/holdtime—Displays how often hello messages are sent on the failover link and how long to wait before testing the peer for failure if no hello messages are received.
- Interface Poll frequency—Displays the interval, in seconds, between hello messages on monitored interfaces.
- Interface Policy—Displays the number of interfaces that must fail before triggering failover.
- Monitored Interfaces—Displays the number of interfaces whose health you are monitoring for failover.
- failover replication http—Displayed if HTTP replication is enabled.
- *Last Failover—Displays the time and date the last failover occurred.
- *This Host(Context)/Other Host(Context)—For each host (or for the selected context in multiple context mode) in the failover pair, the following information is shown:
 - Primary or Secondary—Displays whether the unit is the primary or secondary unit. Also displays the following status:
 - *Active—The unit is the active unit.
 - *Standby—The unit is the standby unit.
 - *Disabled—The unit has failover disabled or the failover link is not configured.
 - *Listen—The unit is attempting to discover an active unit by listening for polling messages.
 - *Learn—The unit detected an active unit, and is not synchronizing the configuration before going to standby mode.
 - *Failed—The unit is failed.

- *Active Time—The amount of time, in seconds, that the unit has been in the active state.
- *[context_name] Interface name (n.n.n.n)—For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions. In multiple context mode, the context name appears before each interface.

Failed—The interface has failed.

Link Down—The interface line protocol is down.

Normal—The interface is working correctly.

No Link—The interface has been administratively shut down.

Unknown—The security appliance cannot determine the status of the interface.

(Waiting)—The interface has not yet received any polling messages from the other unit.

Testing—The interface is being tested.

*Stateful Failover Logical Updates Statistics—The following fields relate to the Stateful Failover feature. If the Link field shows an interface name, then the Stateful Failover statistics are shown.



Note

Stateful Failover is not supported on the ASA 5505 series adaptive security appliance. These statistics do not appear in ASDM running on an ASA 5505 security appliance.

- Link—Displays one of the following:
 - interface_name—The interface used for the Stateful Failover link.
 - Unconfigured—You are not using Stateful Failover.
- Stateful Obj—For each field type, the following statistics are displayed:
 - xmit—Number of transmitted packets to the other unit
 - xerr—Number of errors that occurred while transmitting packets to the other unit
 - rcv—Number of received packets
 - rerr—Number of errors that occurred while receiving packets from the other unit

The following are the stateful object field types:

 - General—Sum of all stateful objects.
 - sys cmd—Logical update system commands; for example, LOGIN and Stay Alive.
 - up time—Up time, which the active unit passes to the standby unit.
 - RPC services—Remote Procedure Call connection information.
 - TCP conn—TCP connection information.
 - UDP conn—Dynamic UDP connection information.
 - ARP tbl—Dynamic ARP table information.
 - L2BRIDGE tbl—Layer 2 bridge table information (transparent firewall mode only).
 - Xlate_Timeout—Indicates connection translation timeout information.
 - VPN IKE upd—IKE connection information.
 - VPN IPSEC upd—IPSec connection information.
 - VPN CTCP upd—cTCP tunnel connection information.
 - VPN SDI upd—SDI AAA connection information.

- VPN DHCP up—Tunneled DHCP connection information.
- *Logical Update Queue Information—Displays the following statistics:
 - Recv Q—The status of the receive queue.
 - Xmit Q—The status of the transmit queue.

The following information is displayed for each queue:

- Cur—The current number of packets in the queue.
- Max—The maximum number of packets.
- Total—The total number of packets.

*Lan-based Failover is active—This field appears only when LAN-based failover is enabled.

- interface name (n.n.n.n) and peer (n.n.n.n)—The name and IP address of the failover link currently being used on each unit.

The following actions are available on the Status pane:

- Make Active—(Only available in Single mode) Click this button to make the security appliance the active unit in an active/standby configuration.
- Make Standby—(Only available in Single mode) Click this button to make the security appliance the standby unit in an active/standby pair.
- Reset Failover—(Only available in Single mode) Click this button to reset a system from the failed state to the standby state. You cannot reset a system to the active state. Clicking this button on the active unit resets the standby unit.
- Reload Standby—(Only available in Single mode) Click this button to force the standby unit to reload.
- Refresh—Click this button to refresh the status information in the Failover state of the system field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

For more information about failover in general, see [Understanding Failover](#).

Graphs

The Graphs pane lets you view failover statistics in graph and table form. In multiple context mode, the Graphs pane is only available in the admin context.

The information in the graphs relate to Stateful Failover only.

Fields

- **Available Graphs for**—Lists the types of statistical information available for monitoring. You can choose up to four statistic types to display in one graph window. Double-clicking a statistic type in this field moves it to the Selected Graphs field. Single-clicking a statistic type in this field selects the entry. You can select multiple entries.

The following types of statistics are available in graph or table format in the graph window. They show the number of packets sent to and received from the other unit in the failover pair.

- **RPC services information**—Displays the security appliance RPC service information.
- **TCP Connection Information**—Displays the security appliance TCP connection information.
- **UDP Connection Information**—Displays the security appliance UDP connection information.
- **ARP Table Information**—Displays the security appliance ARP table information.
- **L2Bridge Table Information**—(Transparent Firewall Mode Only) Displays the layer 2 bridge table packet counts.
- **Xmit Queue**—(Single Mode Only) Displays the current, maximum, and total number of packets transmitted.
- **Receive Queue**—(Single Mode Only) Displays the current, maximum, and total number of packets received.
- **Graph Window**—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- **Add**—Click this button to move the selected entries in the Available Graphs for field to the Selected Graphs field.
- **Remove**—Removes the selected statistic type from the Selected Graphs field.
- **Selected Graphs**—Shows the statistic types you want to show in the selected graph window. You can include up to four types. Double-clicking a statistic type in this field removes the selected statistic type from the field. Single-clicking a statistic type in this field selects the statistic type. You can select multiple statistic types.
- **Show Graphs**—Click this button to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

For more information about failover in general, see [Understanding Failover](#).

Monitoring Failover in the System Execution Space

You can monitor the failover status of the system and of the individual failover groups in the system context. See the following topics for monitoring failover status from the system context:

- [System](#)
- [Failover Group 1 and Failover Group 2](#)

For More Information

For more information about failover in general, see [Understanding Failover](#).

System

The System pane displays the failover state of the system. You can also control the failover state of the system by:

- Toggling the active/standby state of the device.
- Resetting a failed device.
- Reloading the standby unit.

Fields

Failover state of the system—*Display only*. Displays the failover state of the security appliance. The information shown is the same output you would receive from the **show failover** command. The following information is included in the display:

- Failover—Displays “On” when failover is enabled, “Off” when failover is not enabled.
- Cable Status—(PIX security appliance platform only) Displays the status of the serial failover cable. The following shows possible cable states:
 - Normal—The cable is connected to both units, and they both have power.
 - My side not connected—The serial cable is not connected to this unit. It is unknown if the cable is connected to the other unit.
 - Other side is not connected—The serial cable is connected to this unit, but not to the other unit.
 - Other side powered off—The other unit is turned off.
 - N/A—LAN-based failover is enabled.
- Failover unit—Displays the role of the system in the failover pair, either “Primary” or “Secondary”.
- Failover LAN Interface—Displays the logical and physical name of the LAN failover interface. If you are using the dedicated failover cable on the PIX platform, this field displays “N/A - Serial-based failover enabled”. If you have not yet configured the failover interface, this field displays “Not configured”.
- Unit Poll frequency/holdtime—Displays how often hello messages are sent on the failover link and how long to wait before testing the peer for failure if no hello messages are received.
- Interface Poll frequency—Displays the interval, in seconds, between hello messages on monitored interfaces.
- Interface Policy—Displays the number of interfaces that must fail before triggering failover.

- Monitored Interfaces—Displays the number of interfaces whose health you are monitoring for failover.
- failover replication http—Specifies that HTTP replication is enabled.
- Group x Last Failover—Displays the time and date the last failover occurred for each failover group.
- This Host/Other Host —For each host in the failover pair, the following information is shown:
 - Primary or Secondary—Displays whether the unit is the primary or secondary unit.
 - Group x—For each failover group, the following information is shown:
 - State—Active or Standby Ready.
 - Active Time—The amount of time, in seconds, that the failover group has been in the active state.
 - context_name Interface name (n.n.n.n)—For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions.
 - Failed—The interface has failed.
 - Link Down—The interface line protocol is down.
 - Normal—The interface is working correctly.
 - No Link—The interface has been administratively shut down.
 - Unknown—The security appliance cannot determine the status of the interface.
 - (Waiting)—The interface has not yet received any polling messages from the other unit.
 - Testing—The interface is being tested.

Stateful Failover Logical Updates Statistics—The following fields relate to the Stateful Failover feature. If the Link field shows an interface name, then the Stateful Failover statistics are shown.

**Note**

Stateful Failover is not supported on the ASA 5505 series adaptive security appliance. These statistics do not appear in ASDM running on an ASA 5505 security appliance.

- Link—Displays one of the following:
 - *interface_name*—The interface used for the Stateful Failover link.
 - Unconfigured—You are not using Stateful Failover.
- Stateful Obj—For each field type, the following statistics are displayed:
 - xmit—Number of transmitted packets to the other unit
 - xerr—Number of errors that occurred while transmitting packets to the other unit
 - rcv—Number of received packets
 - rerr—Number of errors that occurred while receiving packets from the other unit

The following are the stateful object field types:

 - General—Sum of all stateful objects.
 - sys cmd—Logical update system commands; for example, LOGIN and Stay Alive.
 - up time—Up time, which the active unit passes to the standby unit.
 - RPC services—Remote Procedure Call connection information.
 - TCP conn—TCP connection information.

- UDP conn—Dynamic UDP connection information.
- ARP tbl—Dynamic ARP table information.
- L2BRIDGE tbl—Layer 2 bridge table information (transparent firewall mode only).
- Xlate_Timeout—Indicates connection translation timeout information.
- VPN IKE upd—IKE connection information.
- VPN IPSEC upd—IPSec connection information.
- VPN CTCP upd—cTCP tunnel connection information.
- VPN SDI upd—SDI AAA connection information.
- VPN DHCP upd—Tunneled DHCP connection information.
- Logical Update Queue Information—Displays the following statistics:
 - Recv Q—The status of the receive queue.
 - Xmit Q—The status of the transmit queue.

The following information is displayed for each queue:

- Cur—The current number of packets in the queue.
- Max—The maximum number of packets.
- Total—The total number of packets.

Lan-based Failover is active—This field appears only when LAN-based failover is enabled.

- interface *name (n.n.n.n)* and peer *(n.n.n.n)*—The name and IP address of the failover link currently being used on each unit.

The following actions are available on the System pane:

- Make Active—Click this button to make the security appliance the active unit in an active/standby configuration. In an active/active configuration, clicking this button causes both failover groups to become active on the security appliance.
- Make Standby—Click this button to make the security appliance the standby unit in an active/standby pair. In an active/active configuration, clicking this button causes both failover groups to go to the standby state on the security appliance.
- Reset Failover—Click this button to reset a system from the failed state to the standby state. You cannot reset a system to the active state. Clicking this button on the active unit resets the standby unit.
- Reload Standby—Click this button to force the standby unit to reload.
- Refresh—Click this button to refresh the status information in the Failover state of the system field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	—	—	•

For More Information

For more information about failover in general, see [Understanding Failover](#).

Failover Group 1 and Failover Group 2

The Failover Group 1 and Failover Group 2 panes display the failover state of the selected group. You can also control the failover state of the group by toggling the active/standby state of the group or by resetting a failed group.

Fields

Failover state of Group[x]—*Display only*. Displays the failover state of the selected failover group. The information shown is the same as the output you would receive from the **show failover group** command and contains the following information:

- Last Failover—The time and date of the last failover.
- This Host/Other Host—For each host in the failover pair, the following information is shown:
 - Primary or Secondary—Displays whether the unit is the primary or secondary unit. The following information is also shown for the failover group:
 - Active—The failover group is active on the specified unit.
 - Standby—The failover group is in the standby state on the specified unit.
 - Disabled—The unit has failover disabled or the failover link is not configured.
 - Listen—The unit is attempting to discover an active unit by listening for polling messages.
 - Learn—The unit detected an active unit, and is not synchronizing the configuration before going to standby mode.
 - Failed—The failover group is in the failed state on the specified unit.
 - Active Time—The amount of time, in seconds, that the failover group has been in the active state on the specified unit.
 - *context_name* Interface *name* (n.n.n.n)—For each interface in the selected failover group, the display shows the context to which it belongs and the IP address currently being used on each unit, as well as one of the following conditions.
 - Failed—The interface has failed.
 - Link Down—The interface line protocol is down.
 - Normal—The interface is working correctly.
 - No Link—The interface has been administratively shut down.
 - Unknown—The security appliance cannot determine the status of the interface.
 - (Waiting)—The interface has not yet received any polling messages from the other unit.
 - Testing—The interface is being tested.
- Stateful Failover Logical Updates Statistics—The following fields relate to the Stateful Failover feature. If the Link field shows an interface name, then the Stateful Failover statistics are shown.
 - Link—Displays one of the following:
 - *interface_name*—The interface used for the Stateful Failover link.
 - Unconfigured—You are not using Stateful Failover.
 - Stateful Obj—For each field type, the following statistics are displayed:

- xmit—Number of transmitted packets to the other unit
- xerr—Number of errors that occurred while transmitting packets to the other unit
- rcv—Number of received packets
- rerr—Number of errors that occurred while receiving packets from the other unit

The following are the stateful object field types:

- General—Sum of all stateful objects.
- sys cmd—Logical update system commands; for example, LOGIN and Stay Alive.
- up time—Up time, which the active unit passes to the standby unit.
- RPC services—Remote Procedure Call connection information.
- TCP conn—TCP connection information.
- UDP conn—Dynamic UDP connection information.
- ARP tbl—Dynamic ARP table information.
- L2BRIDGE tbl—Layer 2 bridge table information (transparent firewall mode only).
- Xlate_Timeout—Indicates connection translation timeout information.
- IKE upd—IKE connection information.
- VPN IPSEC upd—IPSec connection information.
- VPN CTCP upd—cTCP tunnel connection information.
- VPN SDI upd—SDI AAA connection information.
- VPN DHCP upd—Tunneled DHCP connection information.
- Logical Update Queue Information—Displays the following statistics:
 - Recv Q—The status of the receive queue.
 - Xmit Q—The status of the transmit queue.

The following information is displayed for each queue:

- Cur—The current number of packets in the queue.
- Max—The maximum number of packets.
- Total—The total number of packets.

You can perform the following actions from this pane:

- Make Active—Click this button to make the failover group active unit on the security appliance.
- Make Standby—Click this button to force the failover group into the standby state on the security appliance.
- Reset Failover—Click this button to reset a system from the failed state to the standby state. You cannot reset a system to the active state. Clicking this button on the active unit resets the standby unit.
- Refresh—Click this button to refresh the status information in the Failover state of the system field.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	—	—	•

For More Information

For more information about failover in general, see [Understanding Failover](#).



CHAPTER 47

Monitoring Trend Micro Content Security



Note

The ASA 5580 does not support the CSC SSM feature.

ASDM lets you monitor the CSC SSM statistics as well as CSC SSM-related features.

For an introduction to the CSC SSM, see [About the CSC SSM](#).



Note

If you have not completed the CSC Setup Wizard in Configuration > Trend Micro Content Security > CSC Setup, you cannot access the panes under Monitoring > Trend Micro Content Security. Instead, a dialog box appears and lets you access the CSC Setup Wizard directly from Monitoring > Trend Micro Content Security.

Threats

The Threats pane lets you view information about various types of threats detected by the CSC SSM in a graph. You can include a maximum of four graphs in one frame. To access this pane, choose **Monitoring > Trend Micro Content Security > Threats**.

Fields

- Available Graphs—Lists the components whose statistics you can view in a graph. The graphs display real-time data in ten-second intervals.
 - Viruses detected—Displays statistics about viruses detected.
 - URL Filtered, URL Blocked—Displays statistics about filtered and blocked URLs.
 - Spam detected—Displays statistics about spam e-mail detected.
 - Spyware blocked—Displays the statistics about blocked spyware.
- Graph Window Title—Shows the graph window name to which you want to add a statistics type. If a graph window is already open, a new graph window is listed by default. To add a statistics type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add more types (a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.

- **Show Graphs**—Click to display a new window that shows a Graph tab and an updated graph with the selected statistics. Click the **Table** tab to display the same information in tabular form.
- From the Graph or Table tab, click **Export** in the menu bar or choose **File > Export** to save the graph or tabular information as a file on your local PC.
- From the Graph or Table tab, click **Print** in the menu bar or choose **File > Print** to print the information displayed in the window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)

Live Security Events

Use the Live Security Events pane to view live, real-time security events in a separate window. To access this pane, choose **Monitoring > Trend Micro Content Security > Live Security Events**.

Fields

- **Buffer Limit**—Displays the maximum number of log messages to view. The default is 1000.
- **View**—Opens a separate window that displays the event messages log. You can pause incoming messages, clear the message window, and save event messages. You can also search messages for specific text.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)

Live Security Events Log

The Live Log dialog box lets you view real-time security event messages that are received from the CSC SSM. You can filter security event messages based on text you specify.

Fields

- Filter By: Choose one of the following from the drop-down list.
 - Show All—Displays all messages.
 - Filter by Text—Lets you filter the messages to view based on text you enter.
- Filter—Click to filter the messages.
- Find Messages—Searches the messages based on the text you enter.
 - Text—Enter the text to search for in the messages log.
 - Find—Click to find the next entry that matches the text you typed in this field.
- Columns—Displays the following, read-only columns:
 - Time—Displays the time an event occurred.
 - Source—Displays the IP address or hostname from which the threat came.
 - Threat/Filter—Displays the type of threat or, in the case of a URL filter event, the filter that triggered the event.
 - Subject/File/URL—Displays the subject of e-mails that contain a threat, the names of FTP files that contain a threat, or blocked or filtered URLs.
 - Receiver/Host—Displays the recipient of e-mails that contain a threat or the IP address or hostname of a threatened node.
 - Sender—Displays the sender of e-mails containing a threat.
 - Content Action—Displays the action taken upon the content of a message, such as cleaning attachments or deleting attachments.
 - Msg Action—Displays the action taken on a message, such as delivering it unchanged, delivering it after deleting the attachments, or delivering it after cleaning the attachments.
- Pause—Click to pause the scrolling of the Live Security Events log.
- Save—Click to save the log to a file on your PC.
- Clear Display—Click to remove the list of messages.
- Close—Click to close the pane and return to the previous screen.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)

Software Updates

The Software Updates pane displays information about updates to the CSC SSM software. This pane refreshes automatically every ten seconds. To access this pane, choose **Monitoring > Trend Micro Content Security > Software Updates**.

Fields

- **Component**—Displays names of parts of the CSC SSM software that can be updated.
- **Version**—Displays the current version of the corresponding component.
- **Last Update**—Displays the date and time that the corresponding component was updated. If the component has never been updated since the CSC SSM software was installed, “None” appears in this column.
- **Last Refresh**—Displays the date and time when ASDM last received information from the CSC SSM about software updates.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)

Resource Graphs

The adaptive security appliance lets you monitor CSC SSM status, including CPU resources and memory usage.

- [CSC CPU, page 47-4](#)
- [CSC Memory, page 47-5](#)

CSC CPU

The CSC CPU pane lets you view information about CPU usage by the CSC SSM in a graph. To access this pane, choose **Monitoring > Trend Micro Content Security > Resource Graphs > CSC CPU**.

Fields

- Available Graphs—Lists the components whose statistics you can view in a graph.
 - CSC CPU, CPU Utilization—Displays statistics for CPU usage on the CSC SSM.
- Graph Window Title—Shows the graph window name to which you want to add a statistics type. If a graph window is already open, a new graph window is listed by default. To add a statistics type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add more types (a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.
- Remove—Click to remove the selected statistics type from the Selected Graphs list.
- Show Graphs—Click to display a new window that shows a Graph tab and an updated graph with the selected statistics. Click the **Table** tab to display the same information in tabular form.
- From the Graph or Table tab, click **Export** in the menu bar or choose **File > Export** to save the graph or tabular information as a file on your local PC.
- From the Graph or Table tab, click **Print** in the menu bar or choose **File > Print** to print the information displayed in the window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)

CSC Memory

The CSC Memory pane lets you view information about memory usage on the CSC SSM in a graph. To access this pane, choose **Monitoring > Trend Micro Content Security > Resource Graphs > CSC Memory**.

Fields

- Available Graphs—Lists the components whose statistics you can view in a graph.
 - Free Memory—Displays statistics about the amount of memory not in use.
 - Used Memory—Displays statistics about the amount of memory in use.
- Graph Window Title—Shows the graph window name to which you want to add a statistics type. If a graph window is already open, a new graph window is listed by default. To add a statistics type to an already open graph, choose the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs list, to which you can add more types (a maximum of four types per window).
- Add—Click to move the selected entries in the Available Graphs For list to the Selected Graphs list.

- **Remove**—Click to remove the selected statistics type from the Selected Graphs list.
- **Show Graphs**—Click to display a new window that shows a Graph tab and an updated graph with the selected statistics. Click the **Table** tab to display the same information in tabular form.
- From the Graph or Table tab, click **Export** in the menu bar or choose **File > Export** to save the graph or tabular information as a file on your local PC.
- From the Graph or Table tab, click **Print** in the menu bar or choose **File > Print** to print the information displayed in the window.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

For More Information

See [Managing the CSC SSM](#)



PART 6

Reference



APPENDIX A

Feature Licenses and Specifications

This appendix describes the feature licenses and specifications. This appendix includes the following sections:

- [Security Appliance and ASDM Release Compatibility, page A-1](#)
- [Client PC Operating System and Browser Requirements, page A-1](#)
- [Supported Platforms and Feature Licenses, page A-2](#)
- [Security Services Module Support, page A-9](#)
- [VPN Specifications, page A-10](#)

Security Appliance and ASDM Release Compatibility

ASDM version 6.1 supports:

- ASA Version 8.1 (available only on the ASA 5580)
- ASA and PIX Version 8.0

Client PC Operating System and Browser Requirements

[Table A-1](#) lists the supported and recommended PC operating systems and browsers for ASDM version 6.1.

Table A-1 *Operating System and Browser Requirements*

Operating System	Version	Browser	Other Requirements
Microsoft Windows ¹	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4)	Internet Explorer 6.0 or 7.0 with Sun Java SE ² Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	SSL Encryption Settings —All available encryption options are enabled for SSL in the browser preferences.
Note	We support both the English and Japanese versions of Windows.	Note	HTTP 1.1 —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.

Table A-1 Operating System and Browser Requirements (continued)

Operating System	Version	Browser	Other Requirements
Apple Macintosh	Apple Macintosh OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0	

1. ASDM is not supported on Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT4.
2. Obtain Sun Java from java.sun.com.

Supported Platforms and Feature Licenses

ASDM version 6.1 supports the following platforms and platform releases; see the associated tables for the feature support for each model:

- ASA 5580, software version 8.1, [Table A-2](#)
- ASA 5505, software version 8.0, [Table A-3](#)
- ASA 5510, software version 8.0, [Table A-4](#)
- ASA 5520, software version 8.0, [Table A-5](#)
- ASA 5540, software version 8.0, [Table A-6](#)
- ASA 5550, software version 8.0, [Table A-7](#)
- PIX 515/515E, software version 8.0, [Table A-8](#)
- PIX 525, software version 8.0, [Table A-9](#)
- PIX 535, software version 8.0, [Table A-10](#)



Note

Items that are in *italics* are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 Clientless SSL VPN license plus the GTP/GPRS license; or all four licenses together.

Table A-2 ASA 5580 Adaptive Security Appliance License Features

ASA 5580	Base License									
Users, concurrent	Unlimited									
Security Contexts	2	Optional licenses:								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and Clientless SSL VPN									
Max. IPSec Sessions	5000									
Max. Clientless SSL VPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									

Table A-2 ASA 5580 Adaptive Security Appliance License Features (continued)

ASA 5580	Base License	
TLS Proxy for SIP and Skinny Inspection	Supported	
Failover	Active/Standby or Active/Active	
GTP/GPRS	None	<i>Optional license: Enabled</i>
Max. VLANs	100	
Concurrent Firewall Conns ²	650 K	
Max. Physical Interfaces	Unlimited	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Min. RAM	4 GB (default)	

- Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-3 ASA 5505 Adaptive Security Appliance License Features in Software Version 8.0

ASA 5505	Base License		Security Plus	
Users, concurrent ¹	10	<i>Optional Licenses:</i>	10	<i>Optional Licenses:</i>
	50	<i>Unlimited</i>	50	<i>Unlimited</i>
Security Contexts	No support		No support	
VPN Sessions ²	10 combined IPSec and Clientless SSL VPN		25 combined IPSec and Clientless SSL VPN	
Max. IPSec Sessions	10		25	
Max. Clientless SSL VPN Sessions	2	<i>Optional License: 10</i>	2	<i>Optional License: 10</i>
VPN Load Balancing	No support		No support	
TLS Proxy for SIP and Skinny Inspection	Supported		Supported	
Failover	No support		Active/Standby (no stateful failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns ³	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Minimum RAM	256 MB (default)		256 MB (default)	

Supported Platforms and Feature Licenses

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit only when they communicate with the outside (Internet VLAN). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host command** to view the host limits.
2. Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
3. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table A-4 ASA 5510 Adaptive Security Appliance License Features in Software Version 8.0

ASA 5510	Base License						Security Plus					
Users, concurrent	Unlimited						Unlimited					
Security Contexts	No support						2	<i>Optional Licenses:</i>				
							5					
VPN Sessions ¹	250 combined IPSec and Clientless SSL VPN						250 combined IPSec and Clientless SSL VPN					
Max. IPSec Sessions	250						250					
Max. Clientless SSL VPN Sessions	2	<i>Optional Licenses:</i>					2	<i>Optional Licenses:</i>				
		10	25	50	100	250		10	25	50	100	250
VPN Load Balancing	No support						No support					
TLS Proxy for SIP and Skinny Inspection	Supported						Supported					
Failover	No support						Active/Standby or Active/Active					
GTP/GPRS	No support						No support					
Max. VLANs	50						100					
Concurrent Firewall Conns ²	50 K						130 K					
Max. Physical Interfaces	Unlimited						Unlimited					
Encryption	Base (DES)		<i>Optional license: Strong (3DES/AES)</i>				Base (DES)		<i>Optional license: Strong (3DES/AES)</i>			
Min. RAM	256 MB (default)						256 MB (default)					

1. Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-5 ASA 5520 Adaptive Security Appliance License Features in Software Version 8.0

ASA 5520	Base License											
Users, concurrent	Unlimited						Unlimited					
Security Contexts	2	<i>Optional Licenses:</i>										
		5	10	20								
VPN Sessions ¹	750 combined IPSec and Clientless SSL VPN											

Table A-5 ASA 5520 Adaptive Security Appliance License Features in Software Version 8.0 (continued)

ASA 5520	Base License									
Max. IPSec Sessions	750									
Max. Clientless SSL VPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750		
VPN Load Balancing	Supported									
TLS Proxy for SIP and Skinny Inspection	Supported									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None		Optional license: Enabled							
Max. VLANs	150									
Concurrent Firewall Conns ²	280 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		Optional license: Strong (3DES/AES)							
Min. RAM	512 MB (default)									

- Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-6 ASA 5540 Adaptive Security Appliance License Features in Software Version 8.0

ASA 5540	Base License									
Users, concurrent	Unlimited						Unlimited			
Security Contexts	2	Optional licenses:								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and Clientless SSL VPN									
Max. IPSec Sessions	5000									
Max. Clientless SSL VPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									
TLS Proxy for SIP and Skinny Inspection	Supported									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None		Optional license: Enabled							
Max. VLANs	200									
Concurrent Firewall Conns ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		Optional license: Strong (3DES/AES)							
Min. RAM	1 GB (default)									

Supported Platforms and Feature Licenses

1. Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-7 ASA 5550 Adaptive Security Appliance License Features in Software Version 8.0

ASA 5550	Base License										
Users, concurrent	Unlimited										
Security Contexts	2	Optional licenses:									
		5	10	20	50						
VPN Sessions ¹	5000 combined IPSec and Clientless SSL VPN										
Max. IPSec Sessions	5000										
Max. Clientless SSL VPN Sessions	2	Optional Licenses:									
		10	25	50	100	250	500	750	1000	2500	5000
VPN Load Balancing	Supported										
TLS Proxy for SIP and Skinny Inspection	Supported										
Failover	Active/Standby or Active/Active										
GTP/GPRS	None		Optional license: Enabled								
Max. VLANs	250										
Concurrent Firewall Conns ²	650 K										
Max. Physical Interfaces	Unlimited										
Encryption	Base (DES)		Optional license: Strong (3DES/AES)								
Min. RAM	4 GB (default)										

1. Although the maximum IPSec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-8 PIX 515/515E Security Appliance License Features in Software Version 8.0

PIX 515/515E	R (Restricted)	UR (Unrestricted)	FO (Failover) ¹	FO-AA (Failover Active/Active) ¹
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
Security Contexts	No support	2 Optional license: 5	2 Optional license: 5	2 Optional license: 5
IPSec Sessions	2000	2000	2000	2000
Clientless SSL VPN Sessions	No support	No support	No support	No support
VPN Load Balancing	No support	No support	No support	No support

Table A-8 PIX 515/515E Security Appliance License Features in Software Version 8.0 (continued)

PIX 515/515E	R (Restricted)			UR (Unrestricted)			FO (Failover) ¹			FO-AA (Failover Active/Active) ¹		
TLS Proxy for SIP and Skinny Inspection	No support			No support			No support			No support		
Failover	No support			Active/Standby Active/Active			Active/Standby			Active/Standby Active/Active		
GTP/GPRS	None	Optional license: Enabled		None	Optional license: Enabled		None	Optional license: Enabled		None	Optional license: Enabled	
Max. VLANs	10			25			25			25		
Concurrent Firewall Conns ²	48 K			130 K			130 K			130 K		
Max. Physical Interfaces	3			6			6			6		
Encryption	None	Optional licenses:		None	Optional licenses:		None	Optional licenses:		None	Optional licenses:	
		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)
Min. RAM	64 MB (default)			128 MB			128 MB			128 MB		

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-9 PIX 525 Security Appliance License Features in Software Version 8.0

PIX 525	R (Restricted)		UR (Unrestricted)				FO (Failover) ¹				FO-AA (Failover Active/Active) ¹						
Users, concurrent	Unlimited		Unlimited				Unlimited				Unlimited						
Security Contexts	No support		2	Optional licenses:				2	Optional licenses:				2	Optional licenses:			
				5	10	20	50		5	10	20	50		5	10	20	50
IPSec Sessions	2000		2000				2000				2000						
Clientless SSL VPN Sessions	No support		No support				No support				No support						
VPN Load Balancing	No support		No support				No support				No support						
TLS Proxy for SIP and Skinny Inspection	No support		No support				No support				No support						
Failover	No support		Active/Standby Active/Active				Active/Standby				Active/Standby Active/Active						
GTP/GPRS	None	Optional license: Enabled	None	Optional license: Enabled			None	Optional license: Enabled			None	Optional license: Enabled					
Max. VLANs	25		100				100				100						

Table A-9 PIX 525 Security Appliance License Features in Software Version 8.0 (continued)

PIX 525	R (Restricted)		UR (Unrestricted)		FO (Failover) ¹		FO-AA (Failover Active/Active) ¹	
Concurrent Firewall Conns ²	140 K		280 K		280 K		280 K	
Max. Physical Interfaces	6		10		10		10	
Encryption	None	Optional licenses:	None	Optional licenses:	None	Optional licenses:	None	Optional licenses:
		Base (DES) Strong (3DES/AES)		Base (DES) Strong (3DES/AES)		Base (DES) Strong (3DES/AES)		Base (DES) Strong (3DES/AES)
Min. RAM	128 MB (default)		256 MB		256 MB		256 MB	

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-10 PIX 535 Security Appliance License Features in Software Version 8.0

PIX 535	R (Restricted)		UR (Unrestricted)		FO (Failover) ¹		FO-AA (Failover Active/Active) ¹	
Users, concurrent	Unlimited		Unlimited		Unlimited		Unlimited	
Security Contexts	No support		2	Optional licenses:	2	Optional licenses:	2	Optional licenses:
				5 10 20 50		5 10 20 50		5 10 20 50
IPSec Sessions	2000		2000		2000		2000	
Clientless SSL VPN Sessions	No support		No support		No support		No support	
VPN Load Balancing	No support		No support		No support		No support	
TLS Proxy for SIP and Skinny Inspection	No support		No support		No support		No support	
Failover	No support		Active/Standby Active/Active		Active/Standby		Active/Standby Active/Active	
GTP/GPRS	None	Optional license: Enabled	None	Optional license: Enabled	None	Optional license: Enabled	None	Optional license: Enabled
Max. VLANs	50		150		150		150	
Concurrent Firewall Conns ²	250 K		500 K		500 K		500 K	
Max. Physical Interfaces	8		14		14		14	

Table A-10 PIX 535 Security Appliance License Features in Software Version 8.0 (continued)

PIX 535	R (Restricted)			UR (Unrestricted)			FO (Failover) ¹			FO-AA (Failover Active/Active) ¹		
Encryption	None	Optional licenses:		None	Optional licenses:		None	Optional licenses:		None	Optional licenses:	
		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)
Min. RAM	512 MB (default)			1024 MB			1024 MB			1024 MB		

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Security Services Module Support

Table A-11 shows the SSMs supported by each platform:

Table A-11 SSM Support

Platform	SSM Models
ASA 5505	No support
ASA 5510	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	AIP SSM 10 AIP SSM 20 CSC SSM 10 ¹ CSC SSM 20 ¹ 4GE SSM
ASA 5550	No support (4GE SSM is built-in and not user-removable)
ASA 5580	No support
PIX 515/515E	No support
PIX 525	No support
PIX 535	No support

1. The CSC SSM licenses support up to 1000 users while the Cisco ASA 5540 Series appliance can support significantly more users. If you deploy CSC SSM with an ASA 5540 adaptive security appliance, be sure to configure the security appliance to send the CSC SSM only the traffic that should be scanned.

VPN Specifications

See the *Cisco ASA 5500 Series VPN Compatibility Reference* at
<http://cisco.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html>.



APPENDIX **B**

Troubleshooting

This appendix describes how to troubleshoot the security appliance, and includes the following sections:

- [Testing Your Configuration, page B-1](#)
- [Reloading the Security Appliance, page B-6](#)
- [Performing Password Recovery, page B-7](#)
- [Using the ROM Monitor to Load a Software Image, page B-10](#)
- [Erasing the Flash File System, page B-11](#)
- [Other Troubleshooting Tools, page B-12](#)
- [Common Problems, page B-13](#)

Testing Your Configuration

This section describes how to test connectivity for the single mode security appliance or for each security context, how to ping the security appliance interfaces, and how to allow hosts on one interface to ping through to hosts on another interface.

We recommend that you only enable pinging and debug messages during troubleshooting. When you are done testing the security appliance, follow the steps in [“Disabling the Test Configuration” section on page B-5](#).

This section includes the following topics:

- [Enabling ICMP Debug Messages and System Log Messages, page B-1](#)
- [Pinging Security Appliance Interfaces, page B-2](#)
- [Pinging Through the Security Appliance, page B-4](#)
- [Disabling the Test Configuration, page B-5](#)

Enabling ICMP Debug Messages and System Log Messages

Debug messages and system log messages can help you troubleshoot why your pings are not successful. The security appliance only shows ICMP debug messages for pings to the security appliance interfaces, and not for pings through the security appliance to other hosts. To enable debugging and system log messages, perform the following steps:

-
- Step 1** To show ICMP packet information for pings to the security appliance interfaces, enter the following command:

```
hostname(config)# debug icmp trace
```

- Step 2** To set system log messages to be sent to Telnet or SSH sessions, enter the following command:

```
hostname(config)# logging monitor debug
```

You can alternately use the **logging buffer debug** command to send log messages to a buffer, and then view them later using the **show logging** command.

- Step 3** To send the system log messages to a Telnet or SSH session, enter the following command:

```
hostname(config)# terminal monitor
```

- Step 4** To enable system log messages, enter the following command:

```
hostname(config)# logging on
```

The following example shows a successful ping from an external host (209.165.201.2) to the security appliance outside interface (209.165.201.1):

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

This example shows the ICMP packet length (32 bytes), the ICMP packet identifier (1), and the ICMP sequence number (the ICMP sequence number starts at 0 and is incremented each time that a request is sent).

Pinging Security Appliance Interfaces

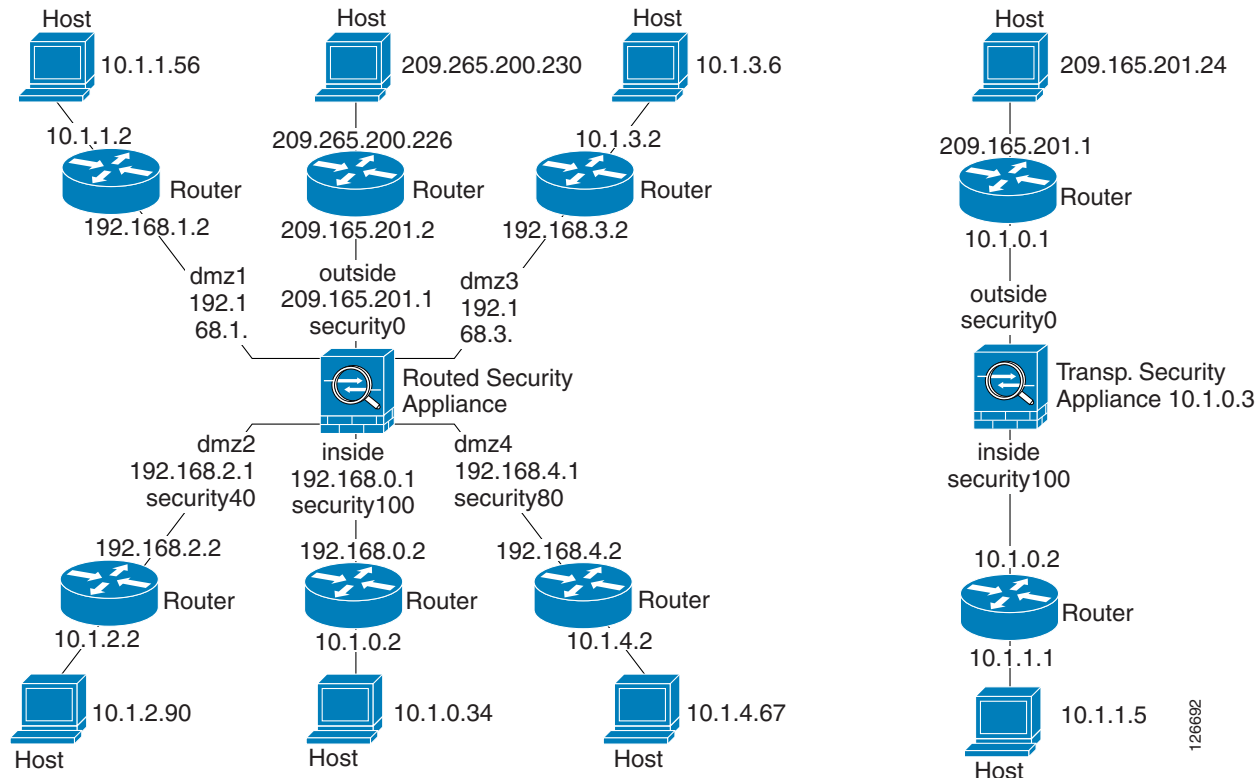
To test whether the security appliance interfaces are up and running and that the security appliance and connected routers are operating correctly, you can ping the security appliance interfaces. To ping the security appliance interfaces, perform the following steps:

-
- Step 1** Draw a diagram of your single-mode security appliance or security context that shows the interface names, security levels, and IP addresses.



Note Although this procedure uses IP addresses, the **ping** command also supports DNS names and names that are assigned to a local IP address with the **name** command.

The diagram should also include any directly connected routers, and a host on the other side of the router from which you will ping the security appliance. You will use this information in this procedure and in the procedure in [“Pinging Through the Security Appliance”](#) section on page B-4. For example:

Figure B-1 Network Diagram with Interfaces, Routers, and Hosts

Step 2 Ping each security appliance interface from the directly connected routers. For transparent mode, ping the management IP address. This test ensures that the security appliance interfaces are active and that the interface configuration is correct.

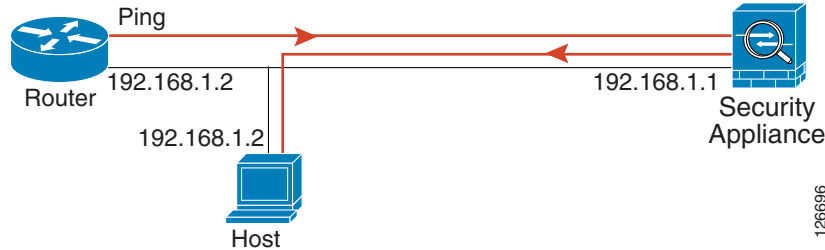
A ping might fail if the security appliance interface is not active, the interface configuration is incorrect, or if a switch between the security appliance and a router is down (see Figure B-2). In this case, no debug messages or system log messages appear, because the packet never reaches the security appliance.

Figure B-2 Ping Failure at Security Appliance Interface

If the ping reaches the security appliance, and the security appliance responds, debug messages similar to the following appear:

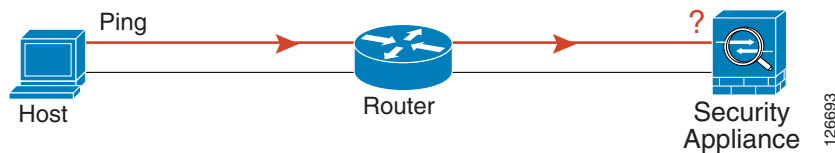
```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

If the ping reply does not return to the router, then a switch loop or redundant IP addresses may exist (see Figure B-3).

Figure B-3 Ping Failure Because of IP Addressing Problems

- Step 3** Ping each security appliance interface from a remote host. For transparent mode, ping the management IP address. This test checks whether the directly connected router can route the packet between the host and the security appliance, and whether the security appliance can correctly route the packet back to the host.

A ping might fail if the security appliance does not have a return route to the host through the intermediate router (see [Figure B-4](#)). In this case, the debug messages show that the ping was successful, but system log message 110001 appears, indicating a routing failure.

Figure B-4 Ping Failure Because the Security Appliance has no Return Route

Pinging Through the Security Appliance

After you successfully ping the security appliance interfaces, make sure traffic can pass successfully through the security appliance. For routed mode, this test shows that NAT is operating correctly, if configured. For transparent mode, which does not use NAT, this test confirms that the security appliance is operating correctly. If the ping fails in transparent mode, contact Cisco TAC.

To ping between hosts on different interfaces, perform the following steps:

- Step 1** To add an access list allowing ICMP from any source host, enter the following command:

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

By default, when hosts access a lower security interface, all traffic is allowed through. However, to access a higher security interface, you need the preceding access list.

- Step 2** To assign the access list to each source interface, enter the following command:

```
hostname(config)# access-group ICMPACL in interface interface_name
```

Repeat this command for each source interface.

- Step 3** To enable the ICMP inspection engine and ensure that ICMP responses may return to the source host, enter the following commands:

```
hostname(config)# class-map ICMP-CLASS
hostname(config-cmap)# match access-list ICMPACL
```

```
hostname(config-cmap) # policy-map ICMP-POLICY
hostname(config-pmap) # class ICMP-CLASS
hostname(config-pmap-c) # inspect icmp
hostname(config-pmap-c) # service-policy ICMP-POLICY global
```

Alternatively, you can also apply the ICMP access list to the destination interface to allow ICMP traffic back through the security appliance.

Step 4 Ping from the host or router through the source interface to another host or router on another interface. Repeat this step for as many interface pairs as you want to check.

If the ping succeeds, a system log message appears to confirm the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter either the **show xlate** or **show conns** command to view this information.

If the ping fails for transparent mode, contact Cisco TAC.

For routed mode, the ping might fail because NAT is not configured correctly (see [Figure B-5](#)). This failure is more likely to occur if you enable NAT control. In this case, a system log message appears, showing that the NAT failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation (required with NAT control), the following system log message appears: “106010: deny inbound icmp.”



Note The security appliance only shows ICMP debug messages for pings to the security appliance interfaces, and not for pings through the security appliance to other hosts.

Figure B-5 Ping Failure Because the Security Appliance is not Translating Addresses



Disabling the Test Configuration

After you complete your testing, disable the test configuration that allows ICMP to and through the security appliance and that prints debug messages. If you leave this configuration in place, it can pose a serious security risk. Debug messages also slow the security appliance performance.

To disable the test configuration, perform the following steps:

Step 1 To disable ICMP debug messages, enter the following command:

```
hostname(config) # no debug icmp trace
```

Step 2 To disable logging, if desired, enter the following command:

```
hostname(config) # no logging on
```

Step 3 To remove the ICMPACL access list, and delete the related **access-group** commands, enter the following command:

```
hostname(config) # no access-list ICMPACL
```

Step 4 (Optional) To disable the ICMP inspection engine, enter the following command:

```
hostname(config)# no service-policy ICMP-POLICY
```

Traceroute

You can trace the route of a packet using the traceroute feature, which is accessed with the **traceroute** command. A traceroute works by sending UDP packets to a destination on an invalid port. Because the port is not valid, the routers along the way to the destination respond with an ICMP Time Exceeded Message, and report that error to the security appliance.

For more information, see [Traceroute](#).

Packet Tracer

In addition, you can trace the lifespan of a packet through the security appliance to see whether the packet is operating correctly with the packet tracer tool. This tool lets you do the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet, along with the CLI commands that caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. If a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. For example, when a packet is dropped because of an invalid header validation, the following message appears: “packet dropped due to bad ip header (reason).”

For more information, see [Packet Tracer](#).

Reloading the Security Appliance

In multiple mode, you can only reload from the system execution space. To reload the security appliance, enter the following command:

```
hostname# reload
```

Recovering from a Lockout

In some circumstances, when you turn on command authorization or CLI authentication, you can be locked out of the security appliance CLI. You can usually recover access by restarting the security appliance. For information on common lockout conditions and how you might recover from them, see

Performing Password Recovery

This section describes how to recover passwords if you have forgotten them or you are locked out because of AAA settings, and how to disable password recovery for extra security. This section includes the following topics:

- [Recovering Passwords for the ASA 5500 Series Adaptive Security Appliance, page B-7](#)
- [Recovering Passwords for the PIX 500 Series Security Appliance, page B-8](#)
- [Disabling Password Recovery, page B-9](#)
- [Using the ROM Monitor to Load a Software Image, page B-10](#)

Recovering Passwords for the ASA 5500 Series Adaptive Security Appliance

To recover passwords for the ASA 5500 Series adaptive security appliance, perform the following steps:

-
- Step 1** Connect to the adaptive security appliance console port.
- Step 2** Power off the adaptive security appliance, and then power it on.
- Step 3** After startup, press the **Escape** key when you are prompted to enter ROMMON mode.
- Step 4** To update the configuration register value, enter the following command:
- ```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```
- Step 5** To set the adaptive security appliance to ignore the startup configuration, enter the following command:
- ```
rommon #1> confreg
```
- The adaptive security appliance displays the current configuration register value, and asks whether you want to change it:
- ```
Current Configuration Register: 0x00000041
Configuration Summary:
 boot default image from Flash
 ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```
- Step 6** Record the current configuration register value, so you can restore it later.
- Step 7** At the prompt, enter **Y** to change the value.
- The adaptive security appliance prompts you for new values.
- Step 8** Accept the default values for all settings. At the prompt, enter **Y**.
- Step 9** Reload the adaptive security appliance by entering the following command:
- ```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```
- The adaptive security appliance loads the default configuration instead of the startup configuration.
- Step 10** Access the privileged EXEC mode by entering the following command:
- ```
hostname> enable
```

- Step 11** When prompted for the password, press **Enter**.  
The password is blank.
- Step 12** Access the global configuration mode by entering the following command:  

```
hostname# configure terminal
```
- Step 13** Change the passwords, as required, in the default configuration by entering the following commands:  

```
hostname(config)# password password
hostname(config)# enable password password
hostname(config)# username name password password
```
- Step 14** Load the default configuration by entering the following command:  

```
hostname(config)# no config-register
```

  
The default configuration register value is 0x1. For more information about the configuration register, see the [Cisco Security Appliance Command Reference](#).
- Step 15** Save the new passwords to the startup configuration by entering the following command:  

```
hostname(config)# copy running-config startup-config
```
- 

## Recovering Passwords for the PIX 500 Series Security Appliance

Recovering passwords on the PIX 500 series security appliance erases the login password, enable password, and **aaa authentication console** commands. To recover passwords for the PIX 500 series security appliance, perform the following steps:

- 
- Step 1** Download the PIX password tool from Cisco.com to a TFTP server accessible from the security appliance. For instructions, go to the following URL:  
[http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products\\_password\\_recovery09186a008009478b.shtml](http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml)
- Step 2** Connect to the security appliance console port.
- Step 3** Power off the security appliance, and then power it on.
- Step 4** Immediately after the startup messages appear, press the **Escape** key to enter monitor mode.
- Step 5** In monitor mode, configure the interface network settings to access the TFTP server by entering the following commands:  

```
monitor> interface interface_id
monitor> address interface_ip
monitor> server tftp_ip
monitor> file pw_tool_name
monitor> gateway gateway_ip
```
- Step 6** Download the PIX password tool from the TFTP server by entering the following command:  

```
monitor> tftp
```

  
If you have trouble reaching the server, enter the **ping address** command to test the connection.
- Step 7** At the “Do you wish to erase the passwords?” prompt, enter **Y**.

You can log in with the default login password of “cisco” and the blank enable password.

The following example shows password recovery on a PIX 500 series security appliance with the TFTP server on the outside interface:

```
monitor> interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7)

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10), MAC: 0050.54ff.82b9
monitor> address 10.21.1.99
address 10.21.1.99
monitor> server 172.18.125.3
server 172.18.125.3
monitor> file np70.bin
file np52.bin
monitor> gateway 10.21.1.1
gateway 10.21.1.1
monitor> ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp np52.bin@172.18.125.3 via 10.21.1.1
Received 73728 bytes

Cisco PIX password tool (4.0) #0: Tue Aug 22 23:22:19 PDT 2005
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000

Do you wish to erase the passwords? [yn] y
Passwords have been erased.

Rebooting....
```

## Disabling Password Recovery

You might want to disable password recovery to ensure that unauthorized users cannot use the password recovery mechanism to compromise the security appliance. To disable password recovery, enter the following command:

```
hostname(config)# no service password-recovery
```

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON mode with the configuration intact. When a user enters ROMMON mode, the security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON mode without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on using ROMMON mode and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to restore the system to an operating state, load a new image and a backup configuration file, if available.

The **service password-recovery** command appears in the configuration file for information only. When you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version

of the command does not change the setting. If you disable password recovery when the security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), then the security appliance changes the setting to load the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to restore the system to an operating state, load a new image and a backup configuration file, if available.

## Using the ROM Monitor to Load a Software Image

This section describes how to load a software image to an adaptive security appliance from the ROM monitor mode using TFTP.

To load a software image to an adaptive security appliance, perform the following steps:

- 
- Step 1** Connect to the adaptive security appliance console port.
  - Step 2** Power off the adaptive security appliance, and then power it on.
  - Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.
  - Step 4** In ROMMON mode, define the interface settings to the adaptive security appliance, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```




---

**Note** Be sure that the connection to the network already exists.

---

- Step 5** To validate your settings, enter the **set** command:

```
rommon #6> set
ROMMON Variable Settings:
 ADDRESS=10.132.44.177
 SERVER=10.129.0.30
 GATEWAY=10.132.44.1
 PORT=Ethernet0/0
 VLAN=untagged
 IMAGE=f1/asa800-232-k8.bin
 CONFIG=
 LINKTIMEOUT=20
 PKTTIMEOUT=4
 RETRY=20
```

- Step 6** Ping the TFTP server by entering the **ping server** command.

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

- Step 7** Load the software image by entering the **tftp** command.

```
rommon #8> tftp
ROMMON Variable Settings:
 ADDRESS=10.132.44.177
 SERVER=10.129.0.30
 GATEWAY=10.132.44.1
 PORT=Ethernet0/0
 VLAN=untagged
 IMAGE=f1/asa800-232-k8.bin
 CONFIG=
 LINKTIMEOUT=20
 PKTTIMEOUT=4
 RETRY=20

tftp f1/asa800-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco PIX Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2007

Loading...
```

After the software image is successfully loaded, the adaptive security appliance automatically exits ROMMON mode.

- Step 8** To verify that the correct software image has been loaded into the adaptive security appliance, check the version in the adaptive security appliance by entering the following command:

```
hostname> show version
```

---

## Erasing the Flash File System

---

- Step 1** Connect to the adaptive security appliance console port.
- Step 2** Power off the adaptive security appliance, and then power it on.
- Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.
- Step 4** To erase the file system, enter the **erase** command, which overwrites all files and erases the file system, including hidden system files.

```
rommon #1> erase [disk0: | disk1: | flash:]
```

---



## Other Troubleshooting Tools

The security appliance provides other troubleshooting tools that you can use. This section includes the following topics:

- [Viewing Debug Messages, page B-12](#)
- [Capturing Packets, page B-12](#)
- [Viewing the Crash Dump, page B-12](#)
- [TACACS+ Server Lockout, page B-12](#)
- [Verifying that Server Authentication and Authorization are Working, page B-12](#)
- [User's Identity not Preserved Across Contexts, page B-13](#)

### Viewing Debug Messages

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of less network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use. To enable debug messages, see the **debug** commands in the [Cisco Security Appliance Command Reference](#).

### Capturing Packets

Capturing packets is sometimes useful when troubleshooting connectivity problems or monitoring suspicious activity. We recommend contacting Cisco TAC if you want to use the packet capture feature. See the **capture** command in the [Cisco Security Appliance Command Reference](#).

### Viewing the Crash Dump

If the security appliance crashes, you can view the crash dump information. We recommend contacting Cisco TAC if you want to interpret the crash dump. See the **show crashdump** command in the [Cisco Security Appliance Command Reference](#).

### TACACS+ Server Lockout

We recommend that, when configuring TACACS+ server command authorization, you do not save your configuration until you are sure it works the way you expect. If you get locked out because of a mistake, you can usually recover access by restarting the security appliance. If you are still locked out, see [Recovering from a Lockout, page 16-32](#).

### Verifying that Server Authentication and Authorization are Working

To verify that the security appliance can contact an AAA server and authenticate or authorize a user, see [Testing Server Authentication and Authorization, page 14-16](#).

## User's Identity not Preserved Across Contexts

If your network will be organized into multiple contexts, be aware that, when changing contexts, the user identity is not preserved. The user becomes a default (enable\_15) user in the new context, with Administrative access (privilege level 15 access).

## Common Problems

This section describes common problems with the security appliance, and how you might resolve them.

**Symptom** ASDM screen becomes blank when you click Configure.

**Possible Cause** CSDM failed due to the data.xml file.

**Recommended Action** Click Refresh.

**Symptom** The context configuration was not saved, and was lost when you reloaded.

**Possible Cause** You did not save each context within the context execution space. If you are configuring contexts at the command line, you did not save the current context before you changed to the next context.

**Recommended Action** Save each context within the context execution space using the **copy run start** command. You cannot save contexts from the system execution space.

**Symptom** You cannot make a Telnet or SSH connection to the security appliance interface.

**Possible Cause** You did not enable Telnet or SSH to the security appliance.

**Recommended Action** Enable Telnet or SSH to the security appliance.

**Symptom** You cannot ping the security appliance interface.

**Possible Cause** You disabled ICMP to the security appliance.

**Recommended Action** Enable ICMP to the security appliance for your IP address using the **icmp** command.

**Symptom** You cannot ping through the security appliance, although the access list allows it.

**Possible Cause** You did not enable the ICMP inspection engine or apply access lists on both the ingress and egress interfaces.

**Recommended Action** Because ICMP is a connectionless protocol, the security appliance does not automatically allow returning traffic through. In addition to an access list on the ingress interface, you either need to apply an access list to the egress interface to allow replying traffic, or enable the ICMP inspection engine, which treats ICMP connections as stateful connections.

**Symptom** Traffic does not pass between two interfaces on the same security level.

**Possible Cause** You did not enable the feature that allows traffic to pass between interfaces at the same security level.

**Recommended Action** Enable this feature.



## CHAPTER **A**

# Configuring an External Server for Authorization and Authentication

---

This appendix describes how to configure an external LDAP or RADIUS server to support the authentication and authorization of security appliance, VPN 3000, and PIX users. Authentication determines who the user is and authorization determines what the user can do. Before you configure the security appliance to use an external server, you must configure the server with the correct security appliance authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.

This appendix includes the following sections:

- [Selecting LDAP, RADIUS, or Local Authentication and Authorization](#)
- [Understanding Policy Enforcement of Permissions and Attributes](#)
- [Configuring an External LDAP Server](#)
- [Configuring an External RADIUS Server](#)

## Selecting LDAP, RADIUS, or Local Authentication and Authorization

To help you decide which authentication or authorization method is right for your platform, this section describes the LDAP and RADIUS support provided with the security appliance (ASA), PIX, and the VPN 3000 platforms.

- **LDAP Authentication**  
Supported on PIX 7.1.x and the security appliance only. VPN 3000 does not support native LDAP authentication. The LDAP server retrieves and searches for the username and enforces any defined attributes as part of the authorization function.
- **LDAP Authorization**  
Supported on PIX, VPN 3000, and the security appliance. The LDAP server retrieves and searches for the username and enforces any defined attributes.
- **RADIUS Authentication**  
Supported on PIX, VPN 3000, and the security appliance. The RADIUS server retrieves and searches for the username and enforces any defined attributes as it performs the authorization function.

- **RADIUS Authorization**  
Supported on PIX, VPN 3000, and the security appliance. The RADIUS server retrieves and searches for the username and enforces any defined attributes.
- **Local Authentication**  
Supported on PIX, VPN 3000, and the security appliance. The Local/Internal server retrieves and searches for the username and enforces any defined attributes as part of the authorization function.
- **Local Authorization**  
Supported on PIX 7.1.x and the security appliance only. The Local/Internal server retrieves and searches for the username and enforces any defined attributes.

## Understanding Policy Enforcement of Permissions and Attributes

You can configure the security appliance to receive user attributes from either the LOCAL/internal database, a RADIUS/LDAP authentication server, or a RADIUS/LDAP authorization server. You can also place users into group-policies with different attributes, but the user attributes will always take precedence. After the device authenticates the user and group(s), the security appliance combines the user and group attribute sets into one aggregate attribute set. The security appliance uses the attributes in the following order and applies the aggregate attribute set to the authenticated user.

1. **User attributes**—The server returns these after successful user authentication or authorization. These take precedence over all others.
2. **Group policy attributes**—These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the 'vpn-group-policy' attribute or from an external RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the format 'OU=GroupName;'. The group policy provides any attributes that are missing from the user attributes. User attributes override group policy attributes if both have a value.
3. **Tunnel group default-group-policy attributes**—These attributes come from the default-group-policy (Base group) that is associated with the tunnel group. After a lookup of that group policy, the Tunnel Group default-group-policy provide any attributes that are missing from the user or group policy attributes. User attributes override group policy attributes if both have a value.
4. **System default attributes**—System default attributes provide any attributes that are missing from the user, group, or tunnel group attributes.

## Configuring an External LDAP Server

**Note**

For more information on the LDAP protocol, see RFCs 1777, 2251, and 2849.

This section describes the structure, schema, and attributes of an LDAP server. It includes the following topics:

- [Reviewing the LDAP Directory Structure and Configuration Procedure](#)
- [Organizing the Security Appliance LDAP Schema](#)
- [Defining the Security Appliance LDAP Schema](#)

- [Loading the Schema in the LDAP Server](#)
- [Defining User Permissions](#)

## Reviewing the LDAP Directory Structure and Configuration Procedure

An LDAP server stores information as entries in a directory. An LDAP schema defines what types of information such entries store. The schema lists classes and the set of required and optional attributes that objects of each class can contain.

To configure your LDAP server to interoperate with the security appliance, define a security appliance authorization schema. A security appliance authorization schema defines the class and attributes of that class that the security appliance supports. Specifically, it comprises the object class (cVPN3000-User-Authorization) and all its possible attributes that may be used to authorize a security appliance user (such as access hours, primary DNS, and so on). Each attribute comprises the attribute name, number (called an object identifier or OID), type, and possible values.

Once you have defined the security appliance authorization schema and loaded it on your server, define the security appliance attributes and permissions and their respective values for each user who will be authorize use of the server.

In summary, to set up your LDAP server:

- Design your security appliance LDAP authorization schema based on the hierarchical set-up of your organization.
- Define the security appliance authorization schema .
- Load the schema on the LDAP server.
- Define permissions for each user on the LDAP server.

The specific steps of these processes vary, depending on which type of LDAP server you are using.

## Organizing the Security Appliance LDAP Schema

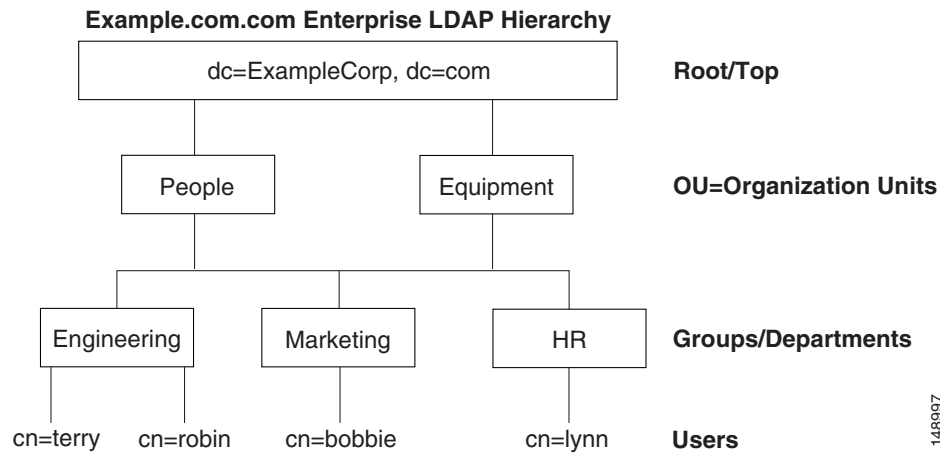
This section describes how to perform searches within the LDAP hierarchy and authenticated binding to the LDAP server on the security appliance. It includes the following topics:

- [Searching the Hierarchy](#)
- [Binding the Security Appliance to the LDAP Server](#)

Before you actually create your schema, think about how your organization is structured. Your LDAP schema should reflect the logical hierarchy of your organization.

For example, suppose an employee at your company, Example Corporation, is named Terry. Terry works in the Engineering group. Your LDAP hierarchy could have one or many levels. You might decide to set up a shallow, single-level hierarchy in which Terry is considered a member of Example Corporation. Or, you could set up a multi-level hierarchy in which Terry is considered to be a member of the department Engineering, which is a member of an organizational unit called People, which is itself a member of Example Corporation. See [Figure C-1](#) for an example of this multi-level hierarchy.

A multi-level hierarchy has more granularity, but a single level hierarchy is quicker to search.

**Figure C-1 A Multi-Level LDAP Hierarchy**

## Searching the Hierarchy

The security appliance lets you tailor the search within the LDAP hierarchy. You configure the following three fields on the security appliance to define where in the LDAP hierarchy your search begins, the extent, and the type of information it is looking for. Together these fields allow you to limit the search of the hierarchy to only the part of the tree that contains the user permissions.

- **LDAP Base DN** defines where in the LDAP hierarchy the server should begin searching for user information when it receives an authorization request from the security appliance.
- **Search Scope** defines the extent of the search in the LDAP hierarchy. The search proceeds this many levels in the hierarchy below the LDAP Base DN. You can choose to have the server search only the level immediately below, or it can search the entire subtree. A single level search is quicker, but a subtree search is more extensive.
- **Naming Attribute(s)** defines the RDN that uniquely identifies an entry in the LDAP server. Common naming attributes are: cn (Common Name) and ui (user identification).

Figure C-1 shows a possible LDAP hierarchy for Example Corporation. Given this hierarchy, you could define your search in different ways. Table C-1 shows two possible search configurations.

In the first example configuration, when Terry establishes the IPSec tunnel with LDAP authorization required, the security appliance sends a search request to the LDAP server indicating it should search for Terry in the Engineering group. This search is quick.

In the second example configuration, the security appliance sends a search request indicating the server should search for Terry within Example Corporation. This search takes longer.

**Table C-1 Example Search Configurations**

| # | LDAP Base DN                                               | Search Scope | Naming Attribute | Result         |
|---|------------------------------------------------------------|--------------|------------------|----------------|
| 1 | group= Engineering,ou=People,dc=ExampleCorporation, dc=com | One Level    | cn=Terry         | Quicker search |
| 2 | dc=ExampleCorporation,dc=com                               | Subtree      | cn=Terry         | Longer search  |

## Binding the Security Appliance to the LDAP Server

Some LDAP servers (including the Microsoft Active Directory server) require the security appliance to establish a handshake via authenticated binding before they accept requests for any other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field defines the authentication characteristics of the security appliance; these characteristics should correspond to those of a user with administrative privileges. An example Login DN field could be: `cn=Administrator, cn=users, ou=people, dc=example, dc=com`.

## Defining the Security Appliance LDAP Schema

This section describes how to define the LDAP schema and AV-pair attribute syntax. It includes the following topics:

- [Cisco-AV-Pair Attribute Syntax](#)
- [Example Security Appliance Authorization Schema](#)

Once you have decided how to structure your user information in the LDAP hierarchy, define this organization in a schema. To define the schema, begin by defining the object class name. The class name for the security appliance directory is `cVPN3000-User-Authorization`. The class has the object identifier (OID) `1.2.840.113556.1.8000.795.1.1`. Every entry or user in the directory is an object of this class.

Some LDAP servers (for example, the Microsoft Active Directory LDAP server) do not allow you to reuse the class OID once you have defined it. Use the next incremental OID. For example, if you incorrectly defined the class name as `cVPN3000-Usr-Authorization` with OID `1.2.840.113556.1.8000.795.1.1`, you can enter the correct class name `cVPN3000-User-Authorization` with the next OID, for example, `1.2.840.113556.1.8000.795.1.2`.

For the Microsoft Active Directory LDAP server, define the schema in text form in a file using the LDAP Data Interchange Format (LDIF). This file has an extension of `.ldif`, for example: `schema.ldif`. Other LDAP servers use graphical user interfaces or script files to define the object class and its attributes. For more information on LDIF, see RFC-2849.

**Note**

All LDAP attributes for all three appliances begin with the letters `cVPN3000`; for example: `cVPN3000-Access-Hours`.

The appliances enforce the LDAP attributes based on attribute name, not numeric ID. RADIUS attributes, on the other hand, are enforced by numeric ID, not by name.

Authorization refers to the process of enforcing permissions or attributes. An LDAP server defined as an authentication or authorization server will enforce permissions or attributes if they are configured.

For a complete list of attributes for the PIX 500 series security appliance and the VPN 3000, see [Table C-2](#).

All strings are case-sensitive and you must use an attribute name as capitalized in the table even if it conflicts with how a term is typically written. For example, use `cVPN3000-IETF-Radius-Class`, not `cVPN3000-IETF-RADIUS-Class`.



**Table C-2** Security Appliance Supported LDAP Cisco Schema Attributes

| Attribute Name/<br>OID (Object Identifier) | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                                                |
|--------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-Access-Hours                      | Y           | Y   | Y   | 1                         | String          | Single                           | Name of the time-range (for example, Business-Hours)                                                                                                           |
| cVPN3000-Simultaneous-Logins               | Y           | Y   | Y   | 2                         | Integer         | Single                           | 0-2147483647                                                                                                                                                   |
| cVPN3000-Primary-DNS                       | Y           | Y   | Y   | 3                         | String          | Single                           | An IP address                                                                                                                                                  |
| cVPN3000-Secondary-DNS                     | Y           | Y   | Y   | 4                         | String          | Single                           | An IP address                                                                                                                                                  |
| cVPN3000-Primary-WINS                      | Y           | Y   | Y   | 5                         | String          | Single                           | An IP address                                                                                                                                                  |
| cVPN3000-Secondary-WINS                    | Y           | Y   | Y   | 6                         | String          | Single                           | An IP address                                                                                                                                                  |
| cVPN3000-SEP-Card-Assignment               |             |     |     | 7                         | Integer         | Single                           | Not used                                                                                                                                                       |
| cVPN3000-Tunneling-Protocols               | Y           | Y   | Y   | 8                         | Integer         | Single                           | 1 = PPTP<br>2 = L2TP<br>4 = IPSec<br>8 = L2TP/IPSec<br>16 = WebVPN.<br>8 and 4 are mutually exclusive<br>(0 - 11, 16 - 27 are legal values)                    |
| cVPN3000-IPSec-Sec-Association             | Y           |     |     | 9                         | String          | Single                           | Name of the security association                                                                                                                               |
| cVPN3000-IPSec-Authentication              | Y           |     |     | 10                        | Integer         | Single                           | 0 = None<br>1 = RADIUS<br>2 = LDAP (authorization only)<br>3 = NT Domain<br>4 = SDI<br>5 = Internal<br>6 = RADIUS with Expiry<br>7 = Kerberos/Active Directory |
| cVPN3000-IPSec-Banner1                     | Y           | Y   | Y   | 11                        | String          | Single                           | Banner string                                                                                                                                                  |
| cVPN3000-IPSec-Allow-Passwd-Store          | Y           | Y   | Y   | 12                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                    |
| cVPN3000-Use-Client-Address                | Y           |     |     | 13                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                    |

**Table C-2**      **Security Appliance Supported LDAP Cisco Schema Attributes (continued)**

| Attribute Name/<br>OID (Object Identifier) | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                           |
|--------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-PPTP-Encryption                   | Y           |     |     | 14                        | Integer         | Single                           | Bitmap:<br>1 = Encryption required<br>2 = 40 bits<br>4 = 128 bits<br>8 = Stateless-Required<br>Example: 15 =<br>40/128-Encr/Stateless-Req |
| cVPN3000-L2TP-Encryption                   | Y           |     |     | 15                        | Integer         | Single                           | Bitmap:<br>1 = Encryption required<br>2 = 40 bit<br>4 = 128 bits<br>8 = Stateless-Req<br>15 =<br>40/128-Encr/Stateless-Req                |
| cVPN3000-IPSec-Split-Tunnel-List           | Y           | Y   | Y   | 16                        | String          | Single                           | Specifies the name of the network or access list that describes the split tunnel inclusion list.                                          |
| cVPN3000-IPSec-Default-Domain              | Y           | Y   | Y   | 17                        | String          | Single                           | Specifies the single default domain name to send to the client (1 - 255 characters).                                                      |
| cVPN3000-IPSec-Split-DNS-Name              | Y           | Y   | Y   | 18                        | String          | Single                           | Specifies the list of secondary domain names to send to the client (1 - 255 characters).                                                  |
| cVPN3000-IPSec-Tunnel-Type                 | Y           | Y   | Y   | 19                        | Integer         | Single                           | 1 = LAN-to-LAN<br>2 = Remote access                                                                                                       |
| cVPN3000-IPSec-Mode-Config                 | Y           | Y   | Y   | 20                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                               |
| cVPN3000-IPSec-User-Group-Lock             | Y           |     |     | 21                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                               |
| cVPN3000-IPSec-Over-UDP                    | Y           | Y   | Y   | 22                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                               |
| cVPN3000-IPSec-Over-UDP-Port               | Y           | Y   | Y   | 23                        | Integer         | Single                           | 4001 - 49151; default = 10000                                                                                                             |
| cVPN3000-IPSec-Banner2                     | Y           | Y   | Y   | 24                        | String          | Single                           | Banner string                                                                                                                             |
| cVPN3000-PPTP-MPPC-Compression             | Y           |     |     | 25                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                               |

**Table C-2**      **Security Appliance Supported LDAP Cisco Schema Attributes (continued)**

| Attribute Name/<br>OID (Object Identifier)        | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                                                                  |
|---------------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-L2TP-MPPC-Compression                    | Y           |     |     | 26                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                      |
| cVPN3000-IPSec-IP-Compression                     | Y           | Y   | Y   | 27                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                      |
| cVPN3000-IPSec-IKE-Peer-ID-Check                  | Y           | Y   | Y   | 28                        | Integer         | Single                           | 1 = Required<br>2 = If supported by peer<br>certificate<br>3 = Do not check                                                                                                      |
| cVPN3000-IKE-Keep-Alives                          | Y           | Y   | Y   | 29                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                      |
| cVPN3000-IPSec-Auth-On-Rekey                      | Y           | Y   | Y   | 30                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                      |
| cVPN3000-Required-Client-<br>Firewall-Vendor-Code | Y           | Y   | Y   | 31                        | Integer         | Single                           | 1 = Cisco Systems (with Cisco<br>Integrated Client)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = Cisco Systems (with Cisco<br>Intrusion Prevention Security<br>Agent) |

**Table C-2** Security Appliance Supported LDAP Cisco Schema Attributes (continued)

| Attribute Name/<br>OID (Object Identifier)         | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-Required-Client-Firewall-Product-Code     | Y           | Y   | Y   | 32                        | Integer         | Single                           | Cisco Systems Products:<br>1 = Cisco Intrusion Prevention Security Agent or Cisco Integrated Client (CIC)<br><br>Zone Labs Products:<br>1 = Zone Alarm<br>2 = Zone AlarmPro<br>3 = Zone Labs Integrity<br><br>NetworkICE Product:<br>1 = BlackIce Defender/Agent<br><br>Sygate Products:<br>1 = Personal Firewall<br>2 = Personal Firewall Pro<br>3 = Security Agent |
| cVPN3000-Required-Client-Firewall-Description      | Y           | Y   | Y   | 33                        | String          | Single                           | String                                                                                                                                                                                                                                                                                                                                                               |
| cVPN3000-Require-Individual-User-Auth              | Y           | Y   | Y   | 34                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                                          |
| cVPN3000-Require-HW-Client-Auth                    | Y           | Y   | Y   | 35                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                                          |
| cVPN3000-Authenticated-User-Idle-Timeout           | Y           | Y   | Y   | 36                        | Integer         | Single                           | 1 - 35791394 minutes                                                                                                                                                                                                                                                                                                                                                 |
| cVPN3000-Cisco-IP-Phone-Bypass                     | Y           | Y   | Y   | 37                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                                                                                                          |
| cVPN3000-IPSec-Split-Tunneling-Policy              | Y           | Y   | Y   | 38                        | Integer         | Single                           | 0 = Tunnel everything<br>1 = Split tunneling<br>2 = Local LAN permitted                                                                                                                                                                                                                                                                                              |
| cVPN3000-IPSec-Required-Client-Firewall-Capability | Y           | Y   | Y   | 39                        | Integer         | Single                           | 0 = None<br>1 = Policy defined by remote FW Are-You-There (AYT)<br>2 = Policy pushed CPP<br>4 = Policy from server                                                                                                                                                                                                                                                   |

**Table C-2** Security Appliance Supported LDAP Cisco Schema Attributes (continued)

| Attribute Name/<br>OID (Object Identifier)     | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                                                                                                                                                                          |
|------------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-IPSec-Client-Firewall-Filter-Name     | Y           |     |     | 40                        | String          | Single                           | Specifies the name of the filter to be pushed to the client as firewall policy.                                                                                                                                                                                                          |
| cVPN3000-IPSec-Client-Firewall-Filter-Optional | Y           | Y   | Y   | 41                        | Integer         | Single                           | 0 = Required<br>1 = Optional                                                                                                                                                                                                                                                             |
| cVPN3000-IPSec-Backup-Servers                  | Y           | Y   | Y   | 42                        | String          | Single                           | 1 = Use Client-Configured list<br>2 = Disabled and clear client list<br>3 = Use Backup Server list                                                                                                                                                                                       |
| cVPN3000-IPSec-Backup-Server-List              | Y           | Y   | Y   | 43                        | String          | Single                           | Server Addresses (space delimited)                                                                                                                                                                                                                                                       |
| cVPN3000-Client-Intercept-DHCP-Configure-Msg   | Y           | Y   | Y   | 44                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                              |
| cVPN3000-MS-Client-Subnet-Mask                 | Y           | Y   | Y   | 45                        | String          | Single                           | An IP address                                                                                                                                                                                                                                                                            |
| cVPN3000-Allow-Network-Extension-Mode          | Y           | Y   | Y   | 46                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                              |
| cVPN3000-Strip-Realm                           | Y           | Y   | Y   | 47                        | Boolean         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                              |
| cVPN3000-Cisco-AV-Pair                         | Y           | Y   | Y   | 48                        | String          | Multi                            | An octet string in the following format:<br><br>[Prefix] [Action] [Protocol]<br>[Source] [Source Wildcard Mask] [Destination]<br>[Destination Wildcard Mask]<br>[Established] [Log] [Operator] [Port]<br><br>For more information, see <a href="#">“Cisco-AV-Pair Attribute Syntax.”</a> |
| cVPN3000-User-Auth-Server-Name                 | Y           |     |     | 49                        | String          | Single                           | IP address or hostname                                                                                                                                                                                                                                                                   |
| cVPN3000-User-Auth-Server-Port                 | Y           |     |     | 50                        | Integer         | Single                           | Port number for server protocol                                                                                                                                                                                                                                                          |
| cVPN3000-User-Auth-Server-Secret               | Y           |     |     | 51                        | String          | Single                           | Server password                                                                                                                                                                                                                                                                          |
| cVPN3000-Confidence-Interval                   | Y           | Y   | Y   | 52                        | Integer         | Single                           | 10 - 300 seconds                                                                                                                                                                                                                                                                         |
| cVPN3000-Cisco-LEAP-Bypass                     | Y           | Y   | Y   | 53                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                                                                                                                                                                                                              |
| cVPN3000-DHCP-Network-Scope                    | Y           | Y   | Y   | 54                        | String          | Single                           | IP address                                                                                                                                                                                                                                                                               |

**Table C-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)**

| Attribute Name/<br>OID (Object Identifier)   | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                                                                                                                            |
|----------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cVPN3000-Client-Type-Version-Limiting        | Y           | Y   | Y   | 55                        | String          | Single                           | IPSec VPN client version number string                                                                                                                                                                     |
| cVPN3000-WebVPN-Content-Filter-Parameters    | Y           | Y   |     | 56                        | Integer         | Single                           | 1 = Java & ActiveX<br>2 = Java scripts<br>4 = Images<br>8 = Cookies in images<br>Add the values to filter multiple parameters. For example: enter 10 to filter both Java scripts and cookies. (10 = 2 + 8) |
| cVPN3000-WebVPN-Enable-functions             |             |     |     | 57                        | Integer         | Single                           | Not used - deprecated                                                                                                                                                                                      |
| cVPN3000-WebVPN-Exchange-Server-Address      |             |     |     | 58                        | String          | Single                           | Not used - deprecated                                                                                                                                                                                      |
| cVPN3000-WebVPN-Exchange-Server-NETBIOS-Name |             |     |     | 59                        | String          | Single                           | Not used - deprecated                                                                                                                                                                                      |
| cVPN3000-Port-Forwarding-Name                | Y           | Y   |     | 60                        | String          | Single                           | Name string (for example, "Corporate-Apps")                                                                                                                                                                |
| cVPN3000-IETF-Radius-Framed-IP-Address       | Y           | Y   | Y   | 61                        | String          | Single                           | An IP address                                                                                                                                                                                              |
| cVPN3000-IETF-Radius-Framed-IP-Netmask       | Y           | Y   | Y   | 62                        | String          | Single                           | An IP address                                                                                                                                                                                              |
| cVPN3000-IETF-Radius-Session-Timeout         | Y           | Y   | Y   | 63                        | Integer         | Single                           | 1 - 35791394 minutes<br>0 = Unlimited                                                                                                                                                                      |
| cVPN3000-IETF-Radius-Idle-Timeout            | Y           | Y   | Y   | 64                        | Integer         | Single                           | 1 - 35791394 minutes<br>0 = Unlimited                                                                                                                                                                      |
| cVPN3000-IETF-Radius-Class                   | Y           | Y   | Y   | 65                        | String          | Single                           | Group name string. Use any of these three formats:<br>OU=Engineering<br>OU=Engineering;<br>Engineering                                                                                                     |
| cVPN3000-IETF-Radius-Filter-Id               | Y           | Y   | Y   | 66                        | String          | Single                           | An access-list                                                                                                                                                                                             |
| cVPN3000-Authorization-Required              | Y           |     |     | 67                        | Integer         | Single                           | 0 = No<br>1 = Yes                                                                                                                                                                                          |
| cVPN3000-Authorization-Type                  | Y           |     |     | 68                        | Integer         | Single                           | 0 = None<br>1 = RADIUS<br>2 = LDAP                                                                                                                                                                         |

**Table C-2 Security Appliance Supported LDAP Cisco Schema Attributes (continued)**

| Attribute Name/<br>OID (Object Identifier)            | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                                                  |
|-------------------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|--------------------------------------------------------------------------------------------------|
| cVPN3000-DN-Field                                     | Y           | Y   | Y   | 69                        | String          | Single                           | Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name. |
| cVPN3000-WebVPN-URL-List                              |             | Y   |     | 70                        | String          | Single                           | URL-list name                                                                                    |
| cVPN3000-WebVPN-Forwarded-Ports                       |             | Y   |     | 71                        | String          | Single                           | Port-Forward list name                                                                           |
| cVPN3000-WebVPN-ACL-Filters                           |             | Y   |     | 72                        | String          | Single                           | Access-List name                                                                                 |
| cVPN3000-WebVPN-Homepage                              | Y           | Y   |     | 73                        | String          | Single                           | A URL such as http://example-portal.com.                                                         |
| cVPN3000-WebVPN-Single-Sign-On-Server-Name            |             | Y   |     | 74                        | String          | Single                           | Name of the SSO Server (1 - 31 characters).                                                      |
| cVPN3000-WebVPN-URL-Entry-Enable                      | Y           | Y   |     | 75                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-File-Access-Enable                    | Y           | Y   |     | 76                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-File-Server-Entry-Enable              | Y           | Y   |     | 77                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-File-Server-Browsing-Enable           | Y           | Y   |     | 78                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Port-Forwarding-Enable                | Y           | Y   |     | 79                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Port-Forwarding-Exchange-Proxy-Enable | Y           | Y   |     | 80                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Port-Forwarding-HTTP-Proxy-Enable     | Y           | Y   |     | 81                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Port-Forwarding-Auto-Download-Enable  | Y           | Y   |     | 82                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Citrix-Support-Enable                 | Y           | Y   |     | 83                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-Apply-ACL-Enable                      | Y           | Y   |     | 84                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-SVC-Enable                            | Y           | Y   |     | 85                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |
| cVPN3000-WebVPN-SVC-Required-Enable                   | Y           | Y   |     | 86                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                                                      |

**Table C-2** Security Appliance Supported LDAP Cisco Schema Attributes (continued)

| Attribute Name/<br>OID (Object Identifier) | VPN<br>3000 | ASA | PIX | Attr.<br>OID <sup>1</sup> | Syntax/<br>Type | Single<br>or<br>Multi-<br>Valued | Possible Values                                                         |
|--------------------------------------------|-------------|-----|-----|---------------------------|-----------------|----------------------------------|-------------------------------------------------------------------------|
| cVPN3000-WebVPN-SVC-Keep-Enable            | Y           | Y   |     | 87                        | Integer         | Single                           | 0 = Disabled<br>1 = Enabled                                             |
| cVPN3000-IE-Proxy-Server                   | Y           |     |     | 88                        | String          | Single                           | IP address                                                              |
| cVPN3000-IE-Proxy-Method                   | Y           |     |     | 89                        | Integer         | Single                           | 1 = No Modify<br>2 = No Proxy<br>3 = Auto Detect<br>4 = Other           |
| cVPN3000-IE-Proxy-Exception-List           | Y           |     |     | 90                        | String          | Single                           | newline (\n)-separated list of<br>DNS domains                           |
| cVPN3000-IE-Proxy-Bypass-Local             | Y           |     |     | 91                        | Integer         | Single                           | 0 = None<br>1 = Local                                                   |
| cVPN3000-Tunnel-Group-Lock                 |             | Y   | Y   | 92                        | String          | Single                           | Name of the tunnel group or<br>"none"                                   |
| cVPN3000-Firewall-ACL-In                   |             | Y   | Y   | 93                        | String          | Single                           | Access list ID                                                          |
| cVPN3000-Firewall-ACL-Out                  |             | Y   | Y   | 94                        | String          | Single                           | Access list ID                                                          |
| cVPN3000-PFS-Required                      | Y           | Y   | Y   | 95                        | Boolean         | Single                           | 0 = No<br>1 = Yes                                                       |
| cVPN3000-WebVPN-SVC-Keepalive              | Y           | Y   |     | 96                        | Integer         | Single                           | 0 = Disabled<br>n = Keepalive value in seconds<br>(15 - 600)            |
| cVPN3000-WebVPN-SVC-Client-DPD             | Y           | Y   |     | 97                        | Integer         | Single                           | 0 = Disabled<br>n = Dead Peer Detection value<br>in seconds (30 - 3600) |
| cVPN3000-WebVPN-SVC-Gateway-DPD            | Y           | Y   |     | 98                        | Integer         | Single                           | 0 = Disabled<br>n = Dead Peer Detection value<br>in seconds (30 - 3600) |
| cVPN3000-WebVPN-SVC-Rekey-Period           | Y           | Y   |     | 99                        | Integer         | Single                           | 0 = Disabled<br>n = Retry period in minutes<br>(4 - 10080)              |
| cVPN3000-WebVPN-SVC-Rekey-Method           | Y           | Y   |     | 100                       | Integer         | Single                           | 0 = None<br>1 = SSL<br>2 = New tunnel<br>3 = Any (sets to SSL)          |
| cVPN3000-WebVPN-SVC-Compression            | Y           | Y   |     | 101                       | Integer         | Single                           | 0 = None<br>1 = Deflate Compression                                     |



1. To get the complete Object Identifier of each attribute, append the number in the column to the end of 1.2.840.113556.8000.795.2. Thus, the OID of the first attribute in the table, cVPN3000-Access-Hours, is 1.2.840.113556.8000.795.2.1. Likewise, the OID of the last attribute in the table, cVPN3000-WebVPN-SVC-Compression, is 1.2.840.113556.8000.795.2.115.

## Cisco-AV-Pair Attribute Syntax

The syntax of each Cisco-AV-Pair rule is as follows:

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

Table C-3 describes the syntax rules.

**Table C-3 AV-Pair Attribute Syntax Rules**

| Field                     | Description                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prefix                    | A unique identifier for the AV pair. For example: <code>ip:inac1#1=</code> (used for standard ACLs) or <code>webvpn:inac1#</code> (used for WebVPN ACLs). This field only appears when the filter has been sent as an AV pair. |
| Action                    | Action to perform if rule matches: <code>deny</code> , <code>permit</code> .                                                                                                                                                   |
| Protocol                  | Number or name of an IP protocol. Either an integer in the range 0 - 255 or one of the following keywords: <code>icmp</code> , <code>igmp</code> , <code>ip</code> , <code>tcp</code> , <code>udp</code> .                     |
| Source                    | Network or host that sends the packet. It is specified as an IP address, a hostname, or the keyword “any”. If specified as an IP address, the source wildcard mask must follow.                                                |
| Source Wildcard Mask      | The wildcard mask applied to the source address.                                                                                                                                                                               |
| Destination               | Network or host that receives the packet. It is specified as an IP address, a hostname, or the keyword “any.” If specified as an IP address, the source wildcard mask must follow.                                             |
| Destination Wildcard Mask | The wildcard mask applied to the destination address.                                                                                                                                                                          |
| Log                       | Generates a FILTER log message. You must use this keyword to generate events of severity level 9.                                                                                                                              |
| Operator                  | Logic operators: greater than, less than, equal to, not equal to.                                                                                                                                                              |
| Port                      | The number of a TCP or UDP port in the range 0 - 65535.                                                                                                                                                                        |

For example:

```
ip:inac1#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
ip:inac1#2=permit TCP any host 10.160.0.1 eq 80 log
```

```
webvpn:inac1#1=permit url http://www.website.com
webvpn:inac1#2=deny smtp any host 10.1.3.5
webvpn:inac1#3=permit url cifs://mar_server/peopleshare1
```

**Note**

Use Cisco-AV pair entries with the `ip:inacl#` prefix to enforce ACLs for remote IPsec and SSL VPN Client (SVC) tunnels.

Use Cisco-AV pair entries with the `webvpn:inacl#` prefix to enforce ACLs for WebVPN clientless (browser-mode) tunnels.

Table C-4 lists the tokens for the Cisco-AV-pair attribute:

**Table C-4 Security Appliance-Supported Tokens**

| Token                          | Syntax Field     | Description                                                                                                                                         |
|--------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip:inacl#Num=</code>     | N/A (Identifier) | (Where <i>Num</i> is a unique integer.) Starts all AV pair access control lists. Enforces ACLs for remote IPsec and SSL VPN (SVC) tunnels.          |
| <code>webvpn:inacl#Num=</code> | N/A (Identifier) | (Where <i>Num</i> is a unique integer.) Starts all WebVPN AV pair access control lists. Enforces ACLs for WebVPN clientless (browser-mode) tunnels. |
| <code>deny</code>              | Action           | Denies action. (Default)                                                                                                                            |
| <code>permit</code>            | Action           | Allows action.                                                                                                                                      |
| <code>icmp</code>              | Protocol         | Internet Control Message Protocol (ICMP)                                                                                                            |
| <code>1</code>                 | Protocol         | Internet Control Message Protocol (ICMP)                                                                                                            |
| <code>IP</code>                | Protocol         | Internet Protocol (IP)                                                                                                                              |
| <code>0</code>                 | Protocol         | Internet Protocol (IP)                                                                                                                              |
| <code>TCP</code>               | Protocol         | Transmission Control Protocol (TCP)                                                                                                                 |
| <code>6</code>                 | Protocol         | Transmission Control Protocol (TCP)                                                                                                                 |
| <code>UDP</code>               | Protocol         | User Datagram Protocol (UDP)                                                                                                                        |
| <code>17</code>                | Protocol         | User Datagram Protocol (UDP)                                                                                                                        |
| <code>any</code>               | Hostname         | Rule applies to any host.                                                                                                                           |
| <code>host</code>              | Hostname         | Any alpha-numeric string that denotes a hostname.                                                                                                   |
| <code>log</code>               | Log              | When the event is hit, a filter log message appears. (Same as permit and log or deny and log.)                                                      |
| <code>lt</code>                | Operator         | Less than value                                                                                                                                     |
| <code>gt</code>                | Operator         | Greater than value                                                                                                                                  |
| <code>eq</code>                | Operator         | Equal to value                                                                                                                                      |
| <code>neq</code>               | Operator         | Not equal to value                                                                                                                                  |
| <code>range</code>             | Operator         | Inclusive range. Should be followed by two values.                                                                                                  |

## Example Security Appliance Authorization Schema

This section provides a sample of an LDAP schema. This schema supports the security appliance class and attributes. It is specific to the Microsoft Active Directory LDAP server. Use it as a model, with Table C-2, to define your own schema for your own LDAP server.

## Schema 3k\_schema.ldif

```

dn:
CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Access-Hours
attributeID: 1.2.840.113556.1.8000.795.2.1
attributeSyntax: 2.5.5.3
cn: cVPN3000-Access-Hours
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Access-Hours
distinguishedName:

CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
 CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Access-Hours
showInAdvancedViewOnly: TRUE

....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
changetype: add
adminDisplayName: cVPN3000-Primary-DNS
attributeID: 1.2.840.113556.1.8000.795.2.3
attributeSyntax: 2.5.5.3
cn: cVPN3000-Primary-DNS
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Primary-DNS
distinguishedName:
CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectCategory:
 CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Primary-DNS
showInAdvancedViewOnly: TRUE

....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation
,DC=com
changetype: add
adminDisplayName: cVPN3000-Confidence-Interval
attributeID: 1.2.840.113556.1.8000.795.2.52
attributeSyntax: 2.5.5.9
cn: cVPN3000-Confidence-Interval
instanceType: 4
isSingleValued: TRUE
LDAPDisplayName: cVPN3000-Confidence-Interval
distinguishedName:

```

```

CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation
,DC=com
objectCategory:

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

dn:
CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
changetype: add
adminDisplayName: cVPN3000-User-Authorization
adminDescription: Cisco Class Schema
cn: cVPN3000-User-Authorization
defaultObjectCategory:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
defaultSecurityDescriptor:
 D: (A;;RPWPCRCDCCLCLOLORCWOWSDDDTDTSW;;;DA) (A;;RPWPCRCDCCLCLOLORCWOWSDDDTDTSW;;;SY)
 (A;;RPLCLORC;;;AU)
governsID: 1.2.840.113556.1.8000.795.1.1
instanceType: 4
LDAPDisplayName: cVPN3000-User-Authorization

mustContain: cn
mayContain: cVPN3000-Access-Hours
mayContain: cVPN3000-Simultaneous-Logins
mayContain: cVPN3000-Primary-DNS
...
mayContain: cVPN3000-Confidence-Interval
mayContain: cVPN3000-Cisco-LEAP-Bypass

distinguishedName:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,
DC=com
objectCategory:
 CN=Class-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: classSchema
objectClassCategory: 1
possSuperiors: organizationalUnit
name: cVPN3000-User-Authorization
rDNAttID: cn
showInAdvancedViewOnly: TRUE
subClassOf: top
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

```

## Loading the Schema in the LDAP Server



### Note

The directions in this section are specific to the Microsoft Active Directory LDAP server. If you have a different type of server, see your server documentation for information on loading a schema.

To load the schema on the LDAP server, enter the following command from the directory where the schema file resides:

```
ldifde -i -f Schema Name
```

For example:

```
ldifde -i -f 3k_schema.ldif
```

## Defining User Permissions



### Note

The directions in this section are specific to the Microsoft Active Directory LDAP server. If you have a different type of server, see your server documentation to define and load user attributes.

For each user authorizing to your LDAP server, define a user file. A user file defines all the security appliance attributes and values associated with a particular user. Each user is an object of the class `cVPN3000-User-Authorization`. To define the user file, use any text editor. The file must have the extension `.ldif`. (For an example user file, see [Robin.ldif](#).)

To load the user file on the LDAP server, enter the following command on the directory where your version of the `ldap_user.ldif` file resides: `ldifde -i -f ldap_user.ldif`. For example: `ldifde -i -f Robin.ldif`

After you have created and loaded both the schema and the user file, your LDAP server is ready to process security appliance authorization requests.

## Example User File

This section provides a sample user file for the user Robin.

### Robin.ldif

```
dn: cn=Robin,OU=People,DC=ExampleCorporation,DC=com
changetype: add
cn: Robin
CVPN3000-Access-Hours: Corporate_time
cVPN3000-Simultaneous-Logins: 2
cVPN3000-IPSec-Over-UDP: TRUE
CVPN3000-IPSec-Over-UDP-Port: 12125
cVPN3000-IPSec-Banner1: Welcome to the Example Corporation!!!
cVPN3000-IPSec-Banner2: Unauthorized access is prohibited!!!!
cVPN3000-Primary-DNS: 10.10.4.5
CVPN3000-Secondary-DNS: 10.11.12.7
CVPN3000-Primary-WINS: 10.20.1.44
CVPN3000-SEP-Card-Assignment: 1
CVPN3000-IPSec-Tunnel-Type: 2
CVPN3000-Tunneling-Protocols: 7
```

```
cVPN3000-Confidence-Interval: 300
cVPN3000-IPSec-Allow-Passwd-Store: TRUE
objectClass: cVPN3000-User-Authorization
```

## Configuring an External RADIUS Server

This section presents an overview of the RADIUS configuration procedure and defines the Cisco RADIUS and TACACS+ attributes. It includes the following topics:

- [Reviewing the RADIUS Configuration Procedure](#)
- [Security Appliance RADIUS Authorization Attributes](#)
- [Security Appliance TACACS+ Attributes](#)

### Reviewing the RADIUS Configuration Procedure

This section describes the RADIUS configuration steps required to support authentication and authorization of the security appliance users. Follow these steps to set up the RADIUS server to interoperate with the security appliance.

- 
- Step 1** Load the security appliance attributes into the RADIUS server. The method you use to load the attributes depends on which type of RADIUS server you are using:
- If you are using Cisco ACS: the server already has these attributes integrated. You can skip this step.
  - If you are using a FUNK RADIUS server: Cisco supplies a dictionary file that contains all the security appliance attributes. Obtain this dictionary file, `cisco3k.dct`, from Software Center on CCO or from the security appliance CD-ROM. Load the dictionary file on your server.
  - For other vendors' RADIUS servers (for example, Microsoft Internet Authentication Service): you must manually define each security appliance attribute. To define an attribute, use the attribute name or number, type, value, and vendor code (3076). For a list of security appliance RADIUS authorization attributes and values, see [Table C-5](#).
- Step 2** Set up the users or groups with the permissions and attributes to send during IPSec/WebVPN tunnel establishment.
- 

### Security Appliance RADIUS Authorization Attributes



#### Note

Authorization refers to the process of enforcing permissions or attributes. A RADIUS server defined as an authentication server enforces permissions or attributes if they are configured.

[Table C-5](#) lists all the possible security appliance supported RADIUS attributes that can be used for user authorization.

**Table C-5** Security Appliance Supported RADIUS Attributes and Values

| Attribute Name           | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                                           |
|--------------------------|----------|-----|-----|---------|-------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access-Hours             | Y        | Y   | Y   | 1       | String      | Single                 | Name of the time range, for example, Business-hours                                                                                                            |
| Simultaneous-Logins      | Y        | Y   | Y   | 2       | Integer     | Single                 | An integer from 0 to 2147483647                                                                                                                                |
| Primary-DNS              | Y        | Y   | Y   | 5       | String      | Single                 | An IP address                                                                                                                                                  |
| Secondary-DNS            | Y        | Y   | Y   | 6       | String      | Single                 | An IP address                                                                                                                                                  |
| Primary-WINS             | Y        | Y   | Y   | 7       | String      | Single                 | An IP address                                                                                                                                                  |
| Secondary-WINS           | Y        | Y   | Y   | 8       | String      | Single                 | An IP address                                                                                                                                                  |
| SEP-Card-Assignment      |          |     |     | 9       | Integer     | Single                 | Not used                                                                                                                                                       |
| Tunneling-Protocols      | Y        | Y   | Y   | 11      | Integer     | Single                 | 1 = PPTP<br>2 = L2TP<br>4 = IPSec<br>8 = L2TP/IPSec<br>16 = WebVPN<br>4 and 8 are mutually exclusive;<br>0-11 and 16-27 are legal values.                      |
| IPSec-Sec-Association    | Y        |     |     | 12      | String      | Single                 | Name of the security association                                                                                                                               |
| IPSec-Authentication     | Y        |     |     | 13      | Integer     | Single                 | 0 = None<br>1 = RADIUS<br>2 = LDAP (authorization only)<br>3 = NT Domain<br>4 = SDI<br>5 = Internal<br>6 = RADIUS with Expiry<br>7 = Kerberos/Active Directory |
| Banner1                  | Y        | Y   | Y   | 15      | String      | Single                 | Banner string                                                                                                                                                  |
| IPSec-Allow-Passwd-Store | Y        | Y   | Y   | 16      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                    |
| Use-Client-Address       | Y        |     |     | 17      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                    |

**Table C-5** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name          | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                             |
|-------------------------|----------|-----|-----|---------|-------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| PPTP-Encryption         | Y        |     |     | 20      | Integer     | Single                 | Bitmap:<br>1 = Encryption required<br>2 = 40 bits<br>4 = 128 bits<br>8 = Stateless-Required<br>15 =<br>40/128-Encr/Stateless-Req |
| L2TP-Encryption         | Y        |     |     | 21      | Integer     | Single                 | Bitmap:<br>1 = Encryption required<br>2 = 40 bit<br>4 = 128 bits<br>8 = Stateless-Req<br>15 =<br>40/128-Encr/Stateless-Req       |
| IPSec-Split-Tunnel-List | Y        | Y   | Y   | 27      | String      | Single                 | Specifies the name of the network or access list that describes the split tunnel inclusion list                                  |
| IPSec-Default-Domain    | Y        | Y   | Y   | 28      | String      | Single                 | Specifies the single default domain name to send to the client (1-255 characters)                                                |
| IPSec-Split-DNS-Names   | Y        | Y   | Y   | 29      | String      | Single                 | Specifies the list of secondary domain names to send to the client (1-255 characters)                                            |
| IPSec-Tunnel-Type       | Y        | Y   | Y   | 30      | Integer     | Single                 | 1 = LAN-to-LAN<br>2 = Remote access                                                                                              |
| IPSec-Mode-Config       | Y        | Y   | Y   | 31      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                      |
| IPSec-User-Group-Lock   | Y        |     |     | 33      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                      |
| IPSec-Over-UDP          | Y        | Y   | Y   | 34      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                      |
| IPSec-Over-UDP-Port     | Y        | Y   | Y   | 35      | Integer     | Single                 | 4001-49151; default = 10000                                                                                                      |
| Banner2                 | Y        | Y   | Y   | 36      | String      | Single                 | A banner string. Banner2 string is concatenated to Banner1 string if configured.                                                 |



**Table C-5** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                       | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                                                    |
|--------------------------------------|----------|-----|-----|---------|-------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PPTP-MPPC-Compression                | Y        |     |     | 37      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                             |
| L2TP-MPPC-Compression                | Y        |     |     | 38      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                             |
| IPSec-IP-Compression                 | Y        | Y   | Y   | 39      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                             |
| IPSec-IKE-Peer-ID-Check              | Y        | Y   | Y   | 40      | Integer     | Single                 | 1 = Required<br>2 = If supported by peer certificate<br>3 = Do not check                                                                                                |
| IKE-Keep-Alives                      | Y        | Y   | Y   | 41      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                             |
| IPSec-Auth-On-Rekey                  | Y        | Y   | Y   | 42      | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                                                             |
| Required-Client-Firewall-Vendor-Code | Y        | Y   | Y   | 45      | Integer     | Single                 | 1 = Cisco Systems (with Cisco Integrated Client)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = Cisco Systems (with Cisco Intrusion Prevention Security Agent) |

**Table C-5**      **Security Appliance Supported RADIUS Attributes and Values (continued)**

| Attribute Name                            | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|----------|-----|-----|---------|-------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Required-Client-Firewall-Product-Code     | Y        | Y   | Y   | 46      | Integer     | Single                 | <p>Cisco Systems Products:</p> <p>1 = Cisco Intrusion Prevention Security Agent or Cisco Integrated Client (CIC)</p> <p>Zone Labs Products:</p> <p>1 = Zone Alarm</p> <p>2 = Zone AlarmPro</p> <p>3 = Zone Labs Integrity</p> <p>NetworkICE Product:</p> <p>1 = BlackIce Defender/Agent</p> <p>Sygate Products:</p> <p>1 = Personal Firewall</p> <p>2 = Personal Firewall Pro</p> <p>3 = Security Agent</p> |
| Required-Client-Firewall-Description      | Y        | Y   | Y   | 47      | String      | Single                 | String                                                                                                                                                                                                                                                                                                                                                                                                      |
| Require-HW-Client-Auth                    | Y        | Y   | Y   | 48      | Boolean     | Single                 | <p>0 = Disabled</p> <p>1 = Enabled</p>                                                                                                                                                                                                                                                                                                                                                                      |
| Required-Individual-User-Auth             | Y        | Y   | Y   | 49      | Integer     | Single                 | <p>0 = Disabled</p> <p>1 = Enabled</p>                                                                                                                                                                                                                                                                                                                                                                      |
| Authenticated-User-Idle-Timeout           | Y        | Y   | Y   | 50      | Integer     | Single                 | 1-35791394 minutes                                                                                                                                                                                                                                                                                                                                                                                          |
| Cisco-IP-Phone-Bypass                     | Y        | Y   | Y   | 51      | Integer     | Single                 | <p>0 = Disabled</p> <p>1 = Enabled</p>                                                                                                                                                                                                                                                                                                                                                                      |
| IPSec-Split-Tunneling-Policy              | Y        | Y   | Y   | 55      | Integer     | Single                 | <p>0 = No split tunneling</p> <p>1 = Split tunneling</p> <p>2 = Local LAN permitted</p>                                                                                                                                                                                                                                                                                                                     |
| IPSec-Required-Client-Firewall-Capability | Y        | Y   | Y   | 56      | Integer     | Single                 | <p>0 = None</p> <p>1 = Policy defined by remote FW Are-You-There (AYT)</p> <p>2 = Policy pushed CPP</p> <p>4 = Policy from server</p>                                                                                                                                                                                                                                                                       |
| IPSec-Client-Firewall-Filter-Name         | Y        |     |     | 57      | String      | Single                 | Specifies the name of the filter to be pushed to the client as firewall policy                                                                                                                                                                                                                                                                                                                              |

**Table C-5** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                        | VPN 3000 | ASA | PIX | Attr. # | Syntax/ Type | Single or Multi-Valued | Description or Value                                                                              |
|---------------------------------------|----------|-----|-----|---------|--------------|------------------------|---------------------------------------------------------------------------------------------------|
| IPSec-Client-Firewall-Filter-Optional | Y        | Y   | Y   | 58      | Integer      | Single                 | 0 = Required<br>1 = Optional                                                                      |
| IPSec-Backup-Servers                  | Y        | Y   | Y   | 59      | String       | Single                 | 1 = Use Client-Configured list<br>2 = Disable and clear client list<br>3 = Use Backup Server list |
| IPSec-Backup-Server-List              | Y        | Y   | Y   | 60      | String       | Single                 | Server Addresses (space delimited)                                                                |
| DHCP-Network-Scope                    | Y        | Y   | Y   | 61      | String       | Single                 | IP Address                                                                                        |
| Intercept-DHCP-Configure-Msg          | Y        | Y   | Y   | 62      | Boolean      | Single                 | 0 = Disabled<br>1 = Enabled                                                                       |
| MS-Client-Subnet-Mask                 | Y        | Y   | Y   | 63      | Boolean      | Single                 | An IP address                                                                                     |
| Allow-Network-Extension-Mode          | Y        | Y   | Y   | 64      | Boolean      | Single                 | 0 = Disabled<br>1 = Enabled                                                                       |
| Authorization-Type                    | Y        | Y   | Y   | 65      | Integer      | Single                 | 0 = None<br>1 = RADIUS<br>2 = LDAP                                                                |
| Authorization-Required                | Y        |     |     | 66      | Integer      | Single                 | 0 = No<br>1 = Yes                                                                                 |
| Authorization-DN-Field                | Y        | Y   | Y   | 67      | String       | Single                 | Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name   |
| IKE-KeepAlive-Confidence-Interval     | Y        | Y   | Y   | 68      | Integer      | Single                 | 10-300 seconds                                                                                    |
| WebVPN-Content-Filter-Parameters      | Y        | Y   |     | 69      | Integer      | Single                 | 1 = Java ActiveX<br>2 = Java Script<br>4 = Image<br>8 = Cookies in images                         |
| WebVPN-URL-List                       |          | Y   |     | 71      | String       | Single                 | URL-List name                                                                                     |
| WebVPN-Port-Forward-List              |          | Y   |     | 72      | String       | Single                 | Port-Forward list name                                                                            |
| WebVPN-Access-List                    |          | Y   |     | 73      | String       | Single                 | Access-List name                                                                                  |
| Cisco-LEAP-Bypass                     | Y        | Y   | Y   | 75      | Integer      | Single                 | 0 = Disabled<br>1 = Enabled                                                                       |
| WebVPN-Homepage                       | Y        | Y   |     | 76      | String       | Single                 | A URL such as<br><a href="http://example-portal.com">http://example-portal.com</a>                |

**Table C-5** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                  | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value                                                                                                                  |
|---------------------------------|----------|-----|-----|---------|-------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Client-Type-Version-Limiting    | Y        | Y   | Y   | 77      | String      | Single                 | IPSec VPN version number string                                                                                                       |
| WebVPN-Port-Forwarding-Name     | Y        | Y   |     | 79      | String      | Single                 | String name (example, "Corporate-Apps").<br><br>This text replaces the default string, "Application Access," on the WebVPN home page. |
| IE-Proxy-Server                 | Y        |     |     | 80      | String      | Single                 | IP address                                                                                                                            |
| IE-Proxy-Server-Policy          | Y        |     |     | 81      | Integer     | Single                 | 1 = No Modify<br>2 = No Proxy<br>3 = Auto detect<br>4 = Use Concentrator Setting                                                      |
| IE-Proxy-Exception-List         | Y        |     |     | 82      | String      | Single                 | newline (\n) separated list of DNS domains                                                                                            |
| IE-Proxy-Bypass-Local           | Y        |     |     | 83      | Integer     | Single                 | 0 = None<br>1 = Local                                                                                                                 |
| IKE-Keepalive-Retry-Interval    | Y        | Y   | Y   | 84      | Integer     | Single                 | 2 - 10 seconds                                                                                                                        |
| Tunnel-Group-Lock               |          | Y   | Y   | 85      | String      | Single                 | Name of the tunnel group or "none"                                                                                                    |
| Access-List-Inbound             |          | Y   | Y   | 86      | String      | Single                 | Access list ID                                                                                                                        |
| Access-List-Outbound            |          | Y   | Y   | 87      | String      | Single                 | Access list ID                                                                                                                        |
| Perfect-Forward-Secrecy-Enable  | Y        | Y   | Y   | 88      | Boolean     | Single                 | 0 = No<br>1 = Yes                                                                                                                     |
| NAC-Enable                      | Y        |     |     | 89      | Integer     |                        | 0 = No<br>1 = Yes                                                                                                                     |
| NAC-Status-Query-Timer          | Y        |     |     | 90      | Integer     |                        | 30-1800 seconds                                                                                                                       |
| NAC-Revalidation-Timer          | Y        |     |     | 91      | Integer     |                        | 300-86400 seconds                                                                                                                     |
| NAC-Default-ACL                 | Y        |     |     | 92      | String      |                        | Access list                                                                                                                           |
| WebVPN-URL-Entry-Enable         | Y        | Y   |     | 93      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                           |
| WebVPN-File-Access-Enable       | Y        | Y   |     | 94      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                           |
| WebVPN-File-Server-Entry-Enable | Y        | Y   |     | 95      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled                                                                                                           |

**Table C-5** Security Appliance Supported RADIUS Attributes and Values (continued)

| Attribute Name                          | VPN 3000 | ASA | PIX | Attr. # | Syntax/Type | Single or Multi-Valued | Description or Value        |
|-----------------------------------------|----------|-----|-----|---------|-------------|------------------------|-----------------------------|
| WebVPN-File-Server-Browsing-Enable      | Y        | Y   |     | 96      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Port-Forwarding-Enable           | Y        | Y   |     | 97      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Outlook-Exchange-Proxy-Enable    | Y        | Y   |     | 98      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Port-Forwarding-HTTP-Proxy       | Y        | Y   |     | 99      | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Auto-Applet-Download-Enable      | Y        | Y   |     | 100     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Citrix-Metaframe-Enable          | Y        | Y   |     | 101     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-Apply-ACL                        | Y        | Y   |     | 102     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Enable            | Y        | Y   |     | 103     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Required          | Y        | Y   |     | 104     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| WebVPN-SSL-VPN-Client-Keep-Installation | Y        | Y   |     | 105     | Integer     | Single                 | 0 = Disabled<br>1 = Enabled |
| Strip-Realm                             | Y        | Y   | Y   | 135     | Boolean     | Single                 | 0 = Disabled<br>1 = Enabled |

**Note**

RADIUS attribute names do not contain the cVPN3000 prefix to better reflect support for all three security appliances (VPN 3000, PIX, and the ASA). Cisco Secure ACS 4.x supports this new nomenclature, but attribute names in pre-4.0 ACS releases still include the cVPN3000 prefix. The appliances enforce the RADIUS attributes based on attribute numeric ID, not attribute name. LDAP attributes are enforced by their name, not by the ID.

## Security Appliance TACACS+ Attributes

The security appliance provides support for TACACS+ attributes. TACACS+ separates the functions of authentication, authorization, and accounting. The protocol supports two types of attributes: mandatory and optional. Both the server and client must understand a mandatory attribute, and the mandatory attribute must be applied to the user. An optional attribute may or may not be understood or used.

**Note**

To use TACACS+ attributes, make sure you have enabled AAA services on the NAS.

[Table C-6](#) lists supported TACACS+ authorization response attributes for cut-through-proxy connections. [Table C-7](#) lists supported TACACS+ accounting attributes.

**Table C-6**      **Supported TACACS+ Authorization Response Attributes**

| Attribute | Description                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| acl       | Identifies a locally configured access list to be applied to the connection.                                                                        |
| idletime  | Indicates the amount of inactivity in minutes that is allowed before the authenticated user session is terminated.                                  |
| timeout   | Specifies the absolute amount of time in minutes that authentication credentials remain active before the authenticated user session is terminated. |

**Table C-7**      **Supported TACACS+ Accounting Attributes**

| Attribute    | Description                                                                                                                                                            |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bytes_in     | Specifies the number of input bytes transferred during this connection (stop records only).                                                                            |
| bytes_out    | Specifies the number of output bytes transferred during this connection (stop records only).                                                                           |
| cmd          | Defines the command executed (command accounting only).                                                                                                                |
| disc-cause   | Indicates the numeric code that identifies the reason for disconnecting (stop records only).                                                                           |
| elapsed_time | Defines the elapsed time in seconds for the connection (stop records only).                                                                                            |
| foreign_ip   | Specifies the IP address of the client for tunnel connections. Defines the address on the lowest security interface for cut-through-proxy connections.                 |
| local_ip     | Specifies the IP address that the client connected to for tunnel connections. Defines the address on the highest security interface for cut-through-proxy connections. |
| NAS port     | Contains a session ID for the connection.                                                                                                                              |
| packs_in     | Specifies the number of input packets transferred during this connection.                                                                                              |
| packs_out    | Specifies the number of output packets transferred during this connection.                                                                                             |
| priv-level   | Set to the user's privilege level for command accounting requests or to 1 otherwise.                                                                                   |
| rem_addr     | Indicates the IP address of the client.                                                                                                                                |
| service      | Specifies the service used. Always set to "shell" for command accounting only.                                                                                         |
| task_id      | Specifies a unique task ID for the accounting transaction.                                                                                                             |
| username     | Indicates the name of the user.                                                                                                                                        |





*Beta Draft -- Cisco Confidential*

## INDEX

---

### Numerics

#### 4GE SSM

- connector types [6-2, 7-2](#)
- fiber [6-2, 7-2](#)
- SFP [6-2, 7-2](#)
- support [A-9](#)

#### 802.1Q trunk [6-3, 7-5](#)

---

### A

#### AAA

- about [14-1, 15-1, 16-1](#)
- auditing session traffic [15-49](#)
- authentication
  - CLI access [15-4, 15-5](#)
  - interactive [15-10](#)
  - network access [15-6](#)
- authorization
  - command [15-19](#)
  - network access [14-10](#)
- server
  - adding [15-34](#)
  - supported types [14-13](#)
- web clients [15-11](#)

#### AAA server group, add (group-policy) [36-6](#)

#### ABR

- definition of [10-2](#)

#### Access Control Server [35-24](#)

#### Access Group panel [11-2](#)

- description [11-2](#)
- fields [11-2](#)

#### accounting

- about [14-12](#)

- supported servers [14-12](#)

#### Accounting tab, tunnel group [36-66](#)

#### ACE

- add/edit/paste [36-15](#)
- Extended ACL tab [36-14](#)

#### ACL

- enabling IPSEC authenticated inbound sessions to bypass ACLs [36-80, 39-28](#)
- extended [36-14](#)
- for Clientless SSL VPN [36-41](#)
- standard [36-14](#)

#### ACL Manager

- Add/Edit/Paste ACE [36-15](#)
- dialog box [36-13](#)

#### Active/Active failover

- about [13-2](#)
- command replication [13-2](#)
- configuration synchronization [13-2](#)

#### Active/Standby failover [13-2](#)

#### ActiveX

- object filtering, benefits of [27-6](#)

#### Add/Edit Access Group dialog box [11-3](#)

- description [11-3](#)
- fields [11-3](#)

#### Add/Edit Filtering Entry dialog box [10-9](#)

- description [10-9](#)
- fields [10-9](#)

#### Add/Edit IGMP Join Group dialog box [11-4](#)

- description [11-4](#)
- fields [11-4](#)

#### Add/Edit IGMP Static Group dialog box [11-7](#)

- description [11-7](#)



**Beta Draft -- Cisco Confidential**

- fields [11-7](#)
- Add/Edit Multicast Group dialog box [11-18](#)
  - description [11-18](#)
  - fields [11-18](#)
- Add/Edit Multicast Route dialog box
  - description [11-8](#)
  - fields [11-8](#)
- Add/Edit OSPF Area dialog box [10-5](#)
  - description [10-5](#)
  - fields [10-6](#)
- Add/Edit OSPF Neighbor Entry dialog box [10-17](#)
  - description [10-17](#)
  - fields [10-18](#)
  - Restrictions [10-17](#)
- Add/Edit Periodic Time Range dialog box [20-16](#)
- Add/Edit Redistribution dialog box [10-16](#)
  - description [10-16](#)
  - fields [10-16](#)
- Add/Edit Rendezvous Point dialog box [11-16](#)
  - description [11-16](#)
  - fields [11-17](#)
  - restrictions [11-17](#)
- Add/Edit Route Summarization dialog box [10-8](#)
  - about [10-8](#)
  - fields [10-8](#)
- Add/Edit SSH Configuration dialog box [17-21](#)
- Add/Edit Summary Address dialog box
  - description [10-19](#)
  - fields [10-19](#)
- Add/Edit Time Range dialog box [20-15](#)
- Add/Edit Virtual Link dialog box [10-20](#)
  - description [10-20](#)
  - fields [10-20](#)
- address assignment, client [36-67](#)
- Address Pool panel, VPN wizard [33-11](#)
- address pools, tunnel group [36-67](#)
- Address Translation Exemption panel, VPN wizard [33-12](#)
- admin context
  - overview [9-1](#)
- administrative access
  - using ICMP for [17-5](#)
- Advanced DHCP Options dialog box [12-7](#)
  - description [12-7](#)
  - fields [12-7](#)
- Advanced OSPF Interface Properties dialog box [10-14](#)
  - description [10-14](#)
  - fields [10-14](#)
- Advanced OSPF Virtual Link Properties dialog box [10-21](#)
  - description [10-21](#)
  - fields [10-21](#)
- Advanced tab, tunnel group [36-67](#)
- AIP SSM
  - about [29-1](#)
  - configuration [29-4](#)
  - sending traffic to [29-6](#)
  - support [A-9](#)
- alternate address, ICMP message [17-52](#)
- APN, GTP application inspection [25-86](#)
- APPE command, denied request [25-80](#)
- application access
  - and e-mail proxy [38-7](#)
  - and Web Access [38-7](#)
  - configuring client applications [38-6](#)
  - enabling cookies on browser [38-6](#)
  - privileges [38-6](#)
  - quitting properly [38-6](#)
  - setting up on client [38-6](#)
  - using e-mail [38-7](#)
  - with IMAP client [38-7](#)
- application firewall [25-93](#)
- application inspection
  - about [25-2](#)
  - applying [25-4](#)
  - configuring [25-4](#)
  - described [25-58](#)
  - enabling for different protocols [25-27](#)
  - security level requirements [6-4, 7-8](#)
- Apply button [1-10](#)

## *Beta Draft -- Cisco Confidential*

- Area/Networks tab [10-5](#)
    - description [10-5](#)
    - fields [10-5](#)
  - area border router [10-2](#)
  - ARP inspection
    - configuring [31-1](#)
  - ARP spoofing [31-2](#)
  - ARP table
    - monitoring [42-1](#)
    - static entry [31-3](#)
  - ASA 5505
    - Base license [8-2](#)
    - client
      - Xauth [36-84](#)
    - MAC addresses [8-4](#)
    - maximum VLANs [8-2](#)
    - power over Ethernet [8-4](#)
    - Security Plus license [8-2](#)
    - SPAN [8-4](#)
  - ASBR
    - definition of [10-2](#)
  - ASDM
    - version [1-14](#)
  - attacks
    - DNS HINFO request [28-15](#)
    - DNS request for all records [28-15](#)
    - DNS zone transfer [28-15](#)
    - DNS zone transfer from high port [28-15](#)
    - fragmented ICMP traffic [28-14](#)
    - IP fragment [28-12](#)
    - IP impossible packet [28-12](#)
    - large ICMP traffic [28-14](#)
    - ping of death [28-14](#)
    - proxied RPC request [28-15](#)
    - statd buffer overflow [28-16](#)
    - TCP FIN only flags [28-15](#)
    - TCP NULL flags [28-14](#)
    - TCP SYN+FIN flags [28-14](#)
    - UDP bomb [28-15](#)
    - UDP chargen DoS [28-15](#)
    - UDP snork [28-15](#)
  - attributes
    - LDAP [C-5](#)
    - policy [C-2](#)
    - RADIUS [C-19](#)
  - Attributes Pushed to Client panel, VPN wizard [33-12](#)
  - attribute-value pairs
    - TACACS+ [C-26](#)
  - auditing session traffic [15-49](#)
  - authenticating a certificate [34-1](#)
  - authentication
    - about [14-1](#)
    - CLI access [15-4, 15-5](#)
    - network access [15-6](#)
    - supported servers [14-4](#)
    - web clients [15-11](#)
  - Authentication tab [10-10](#)
    - description [10-10](#)
    - fields [10-10](#)
  - Authentication tab, tunnel group [36-64](#)
  - authorization
    - about [14-7](#)
    - command [15-19](#)
    - network access [14-10](#)
    - supported servers [14-8](#)
  - Authorization tab, tunnel group [36-65](#)
  - Auto-MDI/MDIX [6-2, 7-2](#)
- 
- ## B
- backed up configurations
    - restoring [2-26](#)
  - backing up configurations [2-25](#)
  - bandwidth [1-16](#)
  - banner, view/configure [36-25](#)
  - Basic tab
    - IPSec LAN-to-LAN, General tab [36-71](#)
  - basic threat detection

**Beta Draft -- Cisco Confidential**

See threat detection

bridging

MAC address table

- learning, disabling [31-6](#)
- overview [31-4](#)
- static entry [31-6](#)

management IP address [5-1](#)

Browse ICMP [36-19](#)

Browse Other [36-20](#)

Browse Source or Destination Address [36-17](#)

Browse Source or Destination Port [36-18](#)

Browse Time Range [36-11](#)

building blocks [20-1](#)

**C**

CA certificate [34-1](#)

CA Certificates [34-1](#)

call agents

- MGCP application inspection [25-107, 25-108](#)

Cancel button [1-10](#)

capturing packets [B-12](#)

CDUP command, denied request [25-80](#)

certificate

- CA [34-1](#)
- code-signer [34-17](#)
- Identity [34-11](#)
- Local CA [34-20](#)

certificate authentication [34-1](#)

certificate enrollment [34-3, 34-12](#)

Cisco-AV-Pair LDAP attributes [C-14](#)

Cisco Client Parameters tab [36-25](#)

Cisco IP Phones, application inspection [25-21](#)

Cisco LDAP attributes [C-5](#)

classes

- See resource management

Client Access Rule, add or edit [36-23](#)

Client Address Assignment [36-67](#)

Client Authentication panel, VPN wizard [33-9](#)

Client Configuration tab [36-24](#)

Client Firewall tab [36-28](#)

Clientless SSL VPN

- client application requirements [38-2](#)
- client requirements [38-2](#)
  - for file management [38-5](#)
  - for network browsing [38-5](#)
  - for web browsing [38-4](#)
- start-up [38-3](#)
- enable cookies for [38-6](#)
- end user set-up [38-1](#)
- printing and [38-3](#)
- remote requirements
  - for port forwarding [38-6](#)
  - for using applications [38-6](#)
- remote system configuration and end-user requirements [38-3](#)
- security tips [38-2](#)
- supported applications [38-2](#)
- supported browsers [38-3](#)
- supported types of Internet connections [38-3](#)
- URL [38-3](#)
- username and password required [38-3](#)
- usernames and passwords [38-1](#)
- use suggestions [38-1](#)

client parameters, configuring [36-24](#)

Client Update, edit , Windows and VPN 3002 clients [36-3](#)

Client Update window, Windows and VPN 3002 clients [36-1](#)

code-signer certificate [34-17](#)

command authorization

- configuring [15-19](#)
- multiple contexts [14-9](#)

configuration

- context files [9-2](#)
- factory default [3-1](#)

configurations, backing up [2-25](#)

Configure IGMP Parameters dialog box [11-5](#)

- description [11-5](#)

## *Beta Draft -- Cisco Confidential*

- fields [11-5](#)
- configuring
  - CSC activation [30-10](#)
  - CSC email [30-22](#)
  - CSC file transfer [30-24](#)
  - CSC IP address [30-11](#)
  - CSC license [30-10](#)
  - CSC management access [30-12](#)
  - CSC notifications [30-11](#)
  - CSC password [30-13](#)
  - CSC Setup Wizard [30-15, 30-19](#)
  - CSC Setup Wizard Activation Codes Configuration [30-15](#)
  - CSC Setup Wizard Host Configuration [30-17](#)
  - CSC Setup Wizard IP Configuration [30-16](#)
  - CSC Setup Wizard Management Access Configuration [30-17](#)
  - CSC Setup Wizard Password Configuration [30-18](#)
  - CSC Setup Wizard Summary [30-20](#)
  - CSC Setup Wizard Traffic Selection for CSC Scan [30-18](#)
  - CSC updates [30-25](#)
  - CSC Web [30-21](#)
- connections per second [1-16](#)
- context mode
  - viewing [1-14](#)
- contexts
  - See security contexts
- conversion error, ICMP message [17-52](#)
- CPU usage [1-15](#)
- crash dump [B-12](#)
- CRL
  - cache refresh time [34-10](#)
  - enforce next update [34-10](#)
- CSC [30-15](#)
- CSC activation
  - configuring [30-10](#)
- CSC CPU
  - monitoring [48-4](#)
- CSC email
  - configuring [30-22](#)
- CSC file transfer
  - configuring [30-24](#)
- CSC File Transfer panel
  - fields [30-24](#)
- CSC IP address
  - configuring [30-11](#)
- CSC license
  - configuring [30-10](#)
- CSC management access
  - configuring [30-12](#)
- CSC memory
  - monitoring [48-5](#)
- CSC notifications
  - configuring [30-11](#)
- CSC password
  - configuring [30-13](#)
- CSC security events
  - monitoring [48-2](#)
- CSC Setup Wizard [30-15](#)
  - activation codes configuration [30-15](#)
  - Host configuration [30-17](#)
  - IP configuration [30-16](#)
  - management access configuration [30-17](#)
  - password configuration [30-18](#)
  - specifying traffic for CSC Scanning [30-19](#)
  - summary [30-20](#)
  - traffic selection for CSC Scan [30-18](#)
- CSC software updates
  - monitoring [48-4](#)
- CSC SSM
  - getting started [30-4](#)
  - overview [30-2](#)
  - support [A-9](#)
  - what to scan [30-6](#)
- CSC threats
  - monitoring [48-1](#)
- CSC updates
  - configuring [30-25](#)

**Beta Draft -- Cisco Confidential**

## CSC Web

configuring [30-21](#)

## CTIQBE

application inspection, enabling [25-27](#)

---

**D**

## data flow

routed firewall [19-1](#)transparent firewall [19-11](#)debug messages [B-12](#)default class [9-12](#)default configuration [3-1](#)default policy [24-2](#)

## default routes

defining equal cost routes [10-41](#)definition of [10-41](#)for tunneled traffic [10-41](#)default tunnel gateway [36-4](#)destination address, browse [36-17](#)destination port, browse [36-18](#)device ID, including in messages [18-6](#)Device Pass-Through [36-85](#)

## DHCP

configuring [12-4](#)interface IP address [8-8](#)

## monitoring

interface lease [42-2](#)IP addresses [42-2](#)server [42-2](#)statistics [42-3](#)services [12-1](#)statistics [42-3](#)

## DHCP relay

overview [12-1](#)DHCP Relay - Add/Edit DHCP Server dialog box [12-3](#)description [12-3](#)fields [12-3](#)restrictions [12-3](#)DHCP Relay panel [12-1](#)description [12-1](#)fields [12-2](#)prerequisites [12-2](#)restrictions [12-1](#)DHCP Server panel [12-4](#)description [12-4](#)fields [12-4](#)DHCP services [12-1](#)digital certificates [34-1](#)directory hierarchy search [C-4](#)disabling content rewrite [39-13](#)

## DNS

application inspection, enabling [25-27](#)

## inspection

about [25-6](#)managing [25-6](#)rewrite, about [25-7](#)NAT effect on [23-13](#)DNS client [12-9](#)DNS HINFO request attack [28-15](#)DNS request for all records attack [28-15](#)DNS zone transfer attack [28-15](#)DNS zone transfer from high port attack [28-15](#)

## duplex

interface [8-13](#)duplex, configuring [6-2, 7-2](#)

## dynamic NAT

*See* NAT

---

**E**

## Easy VPN

## client

Xauth [36-84](#)Easy VPN, advanced properties [36-85](#)Easy VPN client [36-83](#)Easy VPN Remote [36-83](#)echo reply, ICMP message [17-52](#)

## Beta Draft -- Cisco Confidential

### ECMP 10-40

#### Edit DHCP Relay Agent Settings dialog box 12-3

description 12-3

fields 12-3

prerequisites 12-3

restrictions 12-3

#### Edit DHCP Server dialog box 12-6

description 12-6

fields 12-6

#### Edit OSPF Interface Authentication dialog box 10-11

description 10-11

fields 10-11

#### Edit OSPF Interface Properties dialog box 10-13

fields 10-13

#### Edit OSPF Process Advanced Properties dialog box 10-3

description 10-3

fields 10-3

#### Edit PIM Protocol dialog box 11-12

description 11-12

fields 11-12

#### e-mail proxy

and Clientless SSL VPN 38-7

#### Enable IPSec authenticated inbound sessions 36-80, 39-28

#### enrolling

certificate 34-3, 34-12

#### ESMTP

application inspection, enabling 25-27

#### established command, security level requirements 6-5, 7-9

#### Ethernet

Auto-MDI/MDIX 6-2, 7-2

duplex 6-2, 7-2

jumbo frame support

multiple mode 7-7

single mode 6-8

MTU 6-8, 7-10, 8-10

speed 6-2, 7-2

#### extended ACL 36-14

#### external filtering server 27-5

#### External Group Policy, add or edit 36-5

## F

#### factory default configuration 3-1

#### failover

about virtual MAC addresses 13-21

criteria 13-20, 13-28

defining standby IP addresses 13-18, 13-19

defining virtual MAC addresses 13-22

enable 13-26

enabling Active/Standby 13-15

enabling LAN-based 13-15

enabling LAN-based failover 13-26

enabling Stateful Failover 13-16

graphs 47-4

in multiple context mode 13-26

interface

system 7-2

key 13-15, 13-26

make active 47-4

make standby 47-4

monitoring 47-1

monitoring interfaces 13-19

redundant interfaces 6-2, 7-4

reload standby 47-4

reset 47-4, 47-8

stateful 13-3

Stateful Failover 13-27

stateless 13-3

status 47-1

#### failover groups

about 13-29

adding 13-30

editing 13-30

monitoring 47-9

reset 47-10

#### fiber interfaces 6-2, 7-2

#### filtering

benefits of 27-5

rules 27-7

**Beta Draft -- Cisco Confidential**

security level requirements [6-5, 7-8](#)

servers supported [27-1](#)

URLs [27-1](#)

Filtering panel [10-8](#)

benefits [10-8](#)

description [10-8](#)

fields [10-9](#)

restrictions [10-8](#)

firewall, client, configuring settings [36-28](#)

firewall mode

configuring [3-4](#)

overview [19-1](#)

viewing [1-14](#)

firewall server, Zone Labs [36-82](#)

fragmentation policy, IPSec [35-2](#)

fragmented ICMP traffic attack [28-14](#)

FTP

application inspection

enabling [25-28](#)

viewing [24-13, 25-60, 25-62, 25-69, 25-70, 25-77, 25-78, 25-87, 25-88, 25-94, 25-101, 25-104, 25-107, 25-111, 25-113, 25-114, 25-118](#)

filtering option [27-9](#)

FTP inspection

about [25-8](#)

configuring [25-8](#)

---

## G

gateway, default tunnel gateway [36-4](#)

gateways

MGCP application inspection [25-109](#)

General Client Parameters tab [36-24](#)

global addresses

recommendations [23-13](#)

Group Policy window

add or edit, General tab [36-6, 36-10](#)

introduction [36-4](#)

IPSec tab, add or edit [36-21](#)

GTP

application inspection

enabling [25-28](#)

viewing [25-82](#)

GTP inspection

configuring [25-10](#)

---

## H

H.323

transparent firewall guidelines [19-8](#)

H.323 inspection

about [25-12](#)

configuring [25-11](#)

limitations [25-13](#)

H225

application inspection, enabling [25-28](#)

H323 RAS

application inspection, enabling [25-28](#)

Hardware Client tab [36-30](#)

Help button [1-10](#)

HELP command, denied request [25-80](#)

Help menu [1-7](#)

history metrics [5-6](#)

HSRP [19-8](#)

HTTP

application inspection

enabling [25-28](#)

viewing [25-93](#)

filtering [27-1](#)

benefits of [27-6](#)

configuring [27-8](#)

HTTP inspection

configuring [25-13](#)

HTTPS

allowing network or host access to ASDM [17-15](#)

authentication

redirect method [15-10](#)

filtering option [27-9](#)

## Beta Draft -- Cisco Confidential

### I

### ICMP

- add group [36-20](#)
- application inspection, enabling [25-28](#)
- browse [36-19](#)
- rules for access to ADSM [17-5](#)
- testing connectivity [B-1](#)

### ICMP Error

- application inspection, enabling [25-28](#)

### ICMP Group [36-20](#)

### ICMP types

- selecting [17-52](#)

### Identity Certificates [34-11](#)

### IGMP

- access groups [11-2](#)
- configuring interface parameters [11-5](#)
- group membership [11-3](#)
- interface parameters [11-5](#)
- static group assignment [11-6](#)

### IGMP panel

#### IGMP

- overview [11-2](#)

### IKE Policy panel, VPN wizard [33-4](#)

### IKE tunnels, amount [1-15](#)

### ILS

- application inspection, enabling [25-28](#)

### ILS inspection [25-14](#)

### IM [25-20](#)

### information reply, ICMP message [17-52](#)

### information request, ICMP message [17-52](#)

### inspection engines

- See* application inspection

### Instant Messaging inspection [25-20](#)

### interactive authentication [15-10](#)

### interface

- duplex [8-13](#)
- failover link
- system [7-2](#)

### IP address

- DHCP [8-8](#)

### management only [8-8](#)

### MTU [6-8, 7-10, 8-10](#)

### name [8-8](#)

### security level [8-8](#)

### status [1-16](#)

### subinterface, adding [6-5, 7-6](#)

### throughput [1-16](#)

### Interface panel [10-10](#)

### interfaces

#### ASA 5505

- MAC addresses [8-4](#)

- maximum VLANs [8-2](#)

### duplex [6-2, 7-2](#)

### enabled status [7-2](#)

### fiber [6-2, 7-2](#)

### jumbo frame support

- multiple mode [7-7](#)

- single mode [6-8](#)

### monitoring [42-5](#)

### redundant [7-3](#)

### SFP [6-2, 7-2](#)

### speed [6-2, 7-2](#)

### subinterfaces [7-5](#)

### intrusion prevention configuration [29-4](#)

### IP address [5-1](#)

### configuration [8-8](#)

### configuring [8-6](#)

### interface

- DHCP [8-8](#)

### management, transparent firewall [5-1](#)

### IP audit

### enabling [28-10](#)

### monitoring [45-15](#)

### signatures [28-11](#)

### statistics

#### IP audit

### signature matches [45-15](#)



**Beta Draft -- Cisco Confidential**

IP fragment attack [28-12](#)  
 IP fragment database, defaults [28-18](#)  
 IP fragment database, editing [28-19](#)  
 IP impossible packet attack [28-12](#)  
 IP overlapping fragments attack [28-13](#)  
 IPS  
     IP audit [28-10](#)  
 IPS configuration [29-4](#)  
 IPSec  
     Cisco VPN Client [35-9](#)  
     fragmentation policy [35-2](#)  
 IPSec Encryption and Authentication panel, VPN wizard [33-5](#)  
 IPSec tab  
     internal group policy [36-21](#)  
     IPSec LAN-to-LAN [36-73](#)  
     tunnel group [36-68](#)  
 IPSec tunnels, amount [1-15](#)  
 IP teardrop attack [28-13](#)

**J**

Java  
     applet filtering  
         benefits of [27-6](#)  
 Java console [2-12](#)  
 Join Group panel [11-3](#)  
     description [11-3](#)  
     fields [11-4](#)  
 jumbo frame support  
     multiple mode [7-7](#)  
     single mode [6-8](#)

**K**

Kerberos  
     configuring [15-30, 15-38](#)  
     support [14-6](#)  
 key pairs [34-13](#)

**L**

large ICMP traffic attack [28-14](#)  
 Layer 2 firewall  
     *See* transparent firewall  
 Layer 3/4  
     matching multiple policy maps [24-3](#)  
 LDAP  
     AAA support [14-6, 14-11](#)  
     about user authentication [14-6](#)  
     about VPN authorization [14-11](#)  
     application inspection [25-14](#)  
     Cisco attributes [C-5](#)  
     Cisco-AV-pair [C-14](#)  
     configuring [15-31, 15-39](#)  
     configuring a AAA server [C-2 to C-19](#)  
     directory about [C-3](#)  
     directory search [C-4](#)  
     hierarchy example [C-3](#)  
     permissions policy [C-2](#)  
     schema example [C-15](#)  
     schema loading [C-18](#)  
     schema planning [C-3 to C-5](#)  
     server configuration about [C-3](#)  
     user permissions [C-18](#)  
 license [1-15](#)  
 Local CA [34-20](#)  
 Local CA User Database [34-27](#)  
 Local Hosts and Networks panel, VPN wizard [33-6](#)  
 local user database  
     supportAAA  
         local database support [14-4](#)  
 lockout recovery [17-58, B-6](#)  
 logging  
     viewing last 10 messages [1-16](#)  
 LSA  
     about Type 1 [44-1](#)  
     about Type 2 [44-2](#)  
     about Type 3 [44-3](#)

## Beta Draft -- Cisco Confidential

about Type 4 [44-3](#)  
 about Type 5 [44-4](#)  
 about Type 7 [44-4](#)

## M

### MAC address

redundant interfaces [6-3, 7-4](#)

### MAC addresses

ASA 5505 [8-4](#)

### MAC address table [31-4](#)

about [19-11](#)  
 built-in-switch [31-5](#)  
 learning, disabling [31-6](#)  
 monitoring [42-4](#)  
 overview [31-4](#)  
 static entry [31-6](#)

### management traffic [8-8](#)

### man-in-the-middle attack [31-2](#)

### mask reply, ICMP message [17-52](#)

### mask request, ICMP message [17-52](#)

### maximum sessions, IPSec [36-80](#)

### menus [1-4](#)

### MGCP

application inspection  
     configuring [25-109](#)  
     enabling [25-28](#)  
     viewing [25-107](#)

### MGCP inspection

configuring [25-15](#)

### Microsoft client parameters, configuring [36-24](#)

### mobile redirection, ICMP message [17-52](#)

### mode

context [9-9](#)  
 firewall [3-4](#)

### model [1-14](#)

### Modular Policy Framework

*See* MPF

### monitoring

ARP table [42-1](#)

CSC CPU [48-4](#)

CSC memory [48-5](#)

CSC security events [48-2](#)

CSC software updates [48-4](#)

CSC threats [48-1](#)

### DHCP

interface lease [42-2](#)  
 IP addresses [42-2](#)  
 server [42-2](#)  
 statistics [42-3](#)

failover [47-1, 47-6](#)

failover groups [47-9](#)

history metrics [5-6](#)

interfaces [42-5](#)

MAC address table [42-4](#)

routes [44-8](#)

monitoring interfaces [13-19](#)

monitoring switch traffic, ASA 5505 [8-4](#)

### MPF

about [24-1](#)  
 default policy [24-2](#)  
 feature directionality [24-3](#)  
 features [24-1](#)  
 flows [24-3](#)  
 matching multiple policy maps [24-3](#)  
*See also* class map  
*See also* policy map

### MRoute panel [11-11](#)

description [11-7](#)  
 fields [11-7](#)

### MTU [6-8, 7-10, 8-10](#)

### Multicast panel

description [11-1](#)  
 fields [11-1](#)

### Multicast Route panel [11-11](#)

multicast traffic [19-8](#)

multiple mode, enabling [9-9](#)

**N**N2H2 filtering server [27-5](#)name resolution [12-9](#)**NAT**about [23-1](#)application inspection [25-58](#)

bypassing NAT

about [23-10](#)DNS [23-13](#)

dynamic NAT

about [23-6](#)configuring [23-22](#)implementation [23-16](#)

exemption from NAT

about [23-10](#)

identity NAT

about [23-10](#)order of statements [23-13](#)**PAT**about [23-8](#)configuring [23-22](#)implementation [23-16](#)

policy NAT

about [23-10](#)RPC not supported with [25-25](#)same security level [23-12](#)security level requirements [6-5, 7-8](#)

static NAT

about [23-8](#)configuring [23-26](#)

static PAT

about [23-9](#)transparent mode [23-3](#)types [23-6](#)**NETBIOS**application inspection, enabling [25-28](#)

NetBIOS server

tab [36-47](#)

Network Admission Control

uses, requirements, and limitations [35-23](#)New Authentication Server Group panel, VPN wizard [33-10](#)new features [1-1](#)NTLM support [14-11](#)

NT server

configuring [15-29, 15-37](#)support [14-11](#)**O**Options menu [1-5](#)**OSPF**about [10-1](#)adding an LSA filter [10-9](#)authentication settings [10-10](#)authentication support [10-1](#)configuring authentication [10-11](#)defining a static neighbor [10-17](#)defining interface properties [10-13](#)interaction with NAT [10-2](#)interface properties [10-10, 10-12](#)LSA filtering [10-8](#)LSAs [10-2](#)LSA types [44-1](#)monitoring LSAs [44-1](#)neighbor states [44-5](#)route redistribution [10-14](#)static neighbor [10-17](#)summary address [10-18](#)virtual links [10-19](#)

OSPF area

defining [10-5](#)OSPF Neighbors panel [44-5](#)description [44-5](#)fields [44-5](#)

OSPF parameters

dead interval [10-14](#)

## Beta Draft -- Cisco Confidential

hello interval [10-14](#)  
 retransmit interval [10-14](#)  
 transmit delay [10-14](#)  
 OSPF route summarization  
   about [10-7](#)  
   defining [10-8](#)  
 Outlook Web Access (OWA) and Clientless SSL  
 VPN [38-7](#)  
 oversubscribing resources [9-11](#)

## P

packet  
   capture [B-12](#)  
   classifier [9-2](#)  
 packet flow  
   routed firewall [19-1](#)  
   transparent firewall [19-11](#)  
 packet trace, enabling [2-7](#)  
 parameter problem, ICMP message [17-52](#)  
 password  
   Clientless SSL VPN [38-1](#)  
 passwords  
   recovery [B-7](#)  
 PAT  
   *See also* NAT  
 PDP context, GTP application inspection [25-84](#)  
 PIM  
   interface parameters [11-12](#)  
   overview [11-11](#)  
   register message filter [11-18](#)  
   rendezvous points [11-16](#)  
   shortest path tree settings [11-20](#)  
 ping  
   *See* ICMP  
 ping of death attack [28-14](#)  
 platform model [1-14](#)  
 PoE [8-4](#)  
 policy map  
   Layer 3/4  
     feature directionality [24-3](#)  
     flows [24-3](#)  
 policy NAT  
   about [23-10](#)  
 Port Forwarding  
   configuring client applications [38-6](#)  
 port forwarding entry [39-18](#)  
 posture validation  
   uses, requirements, and limitations [35-23](#)  
 Posture Validation Exception, add/edit [35-26](#)  
 power over Ethernet [8-4](#)  
 PPP tab, tunnel-group [36-71](#)  
 PPTP  
   application inspection, enabling [25-28](#)  
 Process Instances tab [10-3](#)  
   description [10-3](#)  
   fields [10-3](#)  
 Properties tab [10-12](#)  
   description [10-12](#)  
   fields [10-12](#)  
 Protocol Group, add [36-21](#)  
 Protocol panel (IGMP) [11-5](#)  
   description [11-5](#)  
   fields [11-5](#)  
 Protocol panel (PIM) [11-12](#)  
   description [11-12](#)  
   fields [11-12](#)  
 proxied RPC request attack [28-15](#)  
 proxy ARP, disabling [10-46](#)  
 proxy bypass [39-22](#)  
 proxy servers  
   SIP and [25-20](#)

## R

RADIUS  
   about authentication support [14-4](#)  
   attribute policy [C-2](#)

**Beta Draft -- Cisco Confidential**

- attributes [C-19](#)
- Cisco AV pair [C-14](#)
- configuring a AAA server [C-19](#)
- configuring a server [15-27](#)
- network access authentication [15-6](#)
- permissions policy [C-2](#)
- RAM, amount
  - memory, amount
    - RAM [1-14](#)
- RealPlayer [25-18](#)
- recurring time range, add or edit [36-13](#)
- redirect, ICMP message [17-52](#)
- redirect method of authentication
  - HTTP
    - authentication
      - redirect method [15-10](#)
- Redistribution panel [10-14](#)
  - description [10-14](#)
  - fields [10-15](#)
- redundant interfaces
  - configuring [7-5](#)
  - failover [6-2, 7-4](#)
  - MAC address [6-3, 7-4](#)
- reloading
  - security appliance [B-6](#)
- Remote Access Client panel, VPN wizard [33-7](#)
- Remote Site Peer panel, VPN wizard [33-3](#)
- Rendezvous Points panel [11-16](#)
  - description [11-16](#)
  - fields [11-16](#)
- Request Filter panel [11-18](#)
  - description [11-18](#)
  - fields [11-18](#)
- reset
  - inbound connections [28-20](#)
  - outside connections [28-20](#)
- Reset button [1-10](#)
- resource management
  - configuring [9-10](#)
  - default class [9-12](#)
  - oversubscribing [9-11](#)
  - overview [9-11](#)
  - unlimited [9-11](#)
- restoring backups [2-26](#)
- rewrite, disabling [39-13](#)
- RIP
  - authentication [10-22](#)
  - definition of [10-22](#)
  - support for [10-22](#)
- RIP panel [10-22](#)
  - fields [10-23](#)
  - limitations [10-22](#)
  - RIP Version 2 Notes [10-22](#)
- RNFR command, denied request [25-80](#)
- RNTO command, denied request [25-80](#)
- routed mode
  - about [19-1](#)
  - setting [3-4](#)
- router advertisement, ICMP message [17-52](#)
- router solicitation, ICMP message [17-52](#)
- Routes panel [44-8](#)
  - description [44-8](#)
  - fields [44-8, 48-4](#)
- Route Summarization tab [10-7](#)
  - about [10-7](#)
  - fields [10-7](#)
- Route Tree panel [11-20](#)
  - description [11-20](#)
  - fields [11-20](#)
- RPC
  - application inspection, enabling [25-29](#)
- RSH
  - application inspection, enabling [25-28](#)
- RTSP
  - application inspection, enabling [25-28](#)
- RTSP inspection
  - about [25-18](#)
  - configuring [25-18](#)

## *Beta Draft -- Cisco Confidential*

### rules

- filtering [27-5](#)
- ICMP [17-6, 17-52](#)

## S

### same security level communication

- NAT [23-12](#)

### SCCP (Skinny) inspection

- about [25-21](#)
- configuration [25-21](#)
- configuring [25-21](#)

### SDI

- configuring [15-29](#)
- support [14-5](#)

### Secure Computing SmartFilter filtering server

- supported [27-1](#)
- URL for website [27-1](#)

### Secure Copy

- about [17-4, 17-49](#)
- configure server [17-27](#)

### Secure Shell dialog box

- description [17-45](#)

### security appliance

- reloading [B-6](#)

### security contexts

- admin context
  - overview [9-1](#)
- cascading [9-7](#)
- classifier [9-2](#)
- command authorization [14-9](#)
- configuration
  - files [9-2](#)
- logging in [9-8](#)
- multiple mode, enabling [9-9](#)
- nesting or cascading [9-8](#)
- overview [9-1](#)
- resource management [9-11](#)
- unsupported features [9-2](#)

### security level

- configuration [8-8](#)

### segment size

- maximum and minimum [28-20](#)

### Server and URL List

- add/edit [36-33](#)

### Server or URL

- dialog box [36-33](#)

### Setup panel [10-2](#)

- about [10-2](#)

### signatures

- attack and informational [28-11](#)

### single mode

- backing up configuration [9-9](#)
- configuration [9-10](#)
- enabling [9-9](#)
- restoring [9-10](#)

### SIP

- application inspection, enabling [25-29](#)

### SIP inspection

- about [25-20](#)
- configuring [25-19](#)
- instant messaging [25-20](#)

### SITE command, denied request [25-80](#)

### Skinny

- application inspection, enabling [25-28](#)

### smart tunnels [39-35](#)

### SMTP inspection [25-23](#)

### SNMP

- application inspection
  - enabling [25-29](#)
  - viewing [25-124](#)
- traps [17-8](#)

### software

- license [1-15](#)
- version [1-14](#)

### source address, browse [36-17](#)

### source port, browse [36-18](#)

### source-quench, ICMP message [17-52](#)

**Beta Draft -- Cisco Confidential**SPAN [8-4](#)specifying traffic for CSC scanning [30-19](#)speed, configuring [6-2, 7-2](#)spoofing, preventing [28-19](#)

SQLNET

application inspection, enabling [25-29](#)

SSM

configuration

AIP SSM [29-4](#)CSC SSM [30-4](#)Standard Access List Rule, add/edit [36-28](#)Standard ACL tab [36-14](#)startup configuration [9-2](#)statd buffer overflow attack [28-16](#)stateful application inspection [25-58](#)Stateful Failover [13-3](#)enabling [13-16](#)Logical Updates Statistics [47-7, 47-9](#)settings [13-27](#)

stateful failover

interface

system [7-2](#)stateless failover [13-3](#)Static Group panel [11-6](#)description [11-6](#)fields [11-6](#)

static NAT

*See* NATStatic Neighbor panel [10-17](#)description [10-17](#)fields [10-17](#)

static PAT

*See* PAT

static routes

about [10-40](#)floating [10-40](#)status bar [1-9](#)

stealth firewall

*See* transparent firewallSTOU command, denied request [25-80](#)

subinterface

adding [6-5, 7-6](#)subinterfaces, adding [7-5](#)subordinate certificate [34-1](#)Summary Address panel [10-18](#)description [10-18](#)fields [10-18](#)Summary panel, VPN wizard [33-7](#)Sun Microsystems Java™ Runtime Environment (JRE)  
and Clientless SSL VPN [38-6](#)Sun Microsystems Java™ Runtime Environment (JRE)  
and WebVPN [39-19](#)

Sun RPC inspection

about [25-25](#)configuring [25-24](#)switch MAC address table [31-5](#)

switch ports

default configuration [8-4](#)SPAN [8-4](#)

system

interface

failover link [7-2](#)

system configuration

network settings [9-2](#)overview [9-1](#)

system messages

device ID, including [18-6](#)viewing last 10 [1-16](#)

---

**T**

TACACS+

about accounting [14-12](#)about authorization [14-11](#)command authorization, configuring [15-21](#)configuring a server group [15-28](#)network access authorization [15-16](#)support [14-5](#)

## *Beta Draft -- Cisco Confidential*

- TCP
  - application inspection [25-58](#)
  - maximum segment size [28-20](#)
  - TIME\_WAIT state [28-20](#)
- TCP FIN only flags attack [28-15](#)
- TCP NULL flags attack [28-14](#)
- TCP Service Group, add [36-18](#)
- TCP SYN+FIN flags attack [28-14](#)
- testing configuration [B-1](#)
- TFTP
  - application inspection, enabling [25-29](#)
- threat detection
  - basic
    - drop types [28-2](#)
    - enabling [28-2](#)
    - overview [28-2](#)
    - rate intervals [28-2](#)
    - system performance [28-2](#)
  - scanning
    - default limits, changing [28-4](#)
    - enabling [28-3](#)
    - host database [28-3](#)
    - overview [28-3](#)
    - shunning attackers [28-4](#)
    - system performance [28-4](#)
  - scanning statistics
    - enabling [28-4](#)
    - system performance [1-17, 28-4, 28-5](#)
- TIME\_WAIT state [28-20](#)
- time exceeded, ICMP message [17-52](#)
- time range
  - add or edit [36-12](#)
  - browse [36-11](#)
  - recurring [36-13](#)
- timestamp reply, ICMP message [17-52](#)
- timestamp request, ICMP message [17-52](#)
- Tools menu [1-6](#)
- traceroute, enabling [1-6, 2-11](#)
- traffic flow
  - routed firewall [19-1](#)
  - transparent firewall [19-11](#)
- traffic usage [1-16](#)
- transparent firewall
  - about [19-7](#)
  - data flow [19-11](#)
  - guidelines [19-9](#)
  - H.323 guidelines [19-8](#)
  - HSRP [19-8](#)
  - MAC address table
    - learning, disabling [31-6](#)
    - overview [31-4](#)
    - static entry [31-6](#)
  - Management 0/0 IP address [6-6, 7-9](#)
  - management IP address [5-1](#)
  - multicast traffic [19-8](#)
  - unsupported features [19-10](#)
  - VRRP [19-8](#)
- transparent mode
  - NAT [23-3](#)
- traps, SNMP [17-8](#)
- trunk, 802.1Q [6-3, 7-5](#)
- Tunneled Management [36-85](#)
- tunnel gateway, default [36-4](#)
- Type 1 panel [44-1](#)
  - description [44-1](#)
  - fields [44-2](#)
- Type 2 panel [44-2](#)
  - description [44-2](#)
  - fields [44-2](#)
- Type 3 panel [44-3](#)
  - description [44-3](#)
  - fields [44-3](#)
- Type 4 panel [44-3](#)
  - description [44-3](#)
  - fields [44-3](#)
- Type 5 panel [44-4](#)
  - description [44-4](#)
  - fields [44-4](#)



**Beta Draft -- Cisco Confidential**Type 7 panel [44-4](#)description [44-4](#)fields [44-5](#)

---

**U****UDP**application inspection [25-58](#)bomb attack [28-15](#)chargen DoS attack [28-15](#)snork attack [28-15](#)Unicast Reverse Path Forwarding [28-19](#)

unreachable messages

ICMP type [17-52](#)required for MTU discovery [17-6, 17-52](#)uptime [1-14](#)**URL**

filtering

benefits of [27-6](#)configuring [27-8](#)**URLs**filtering [27-1](#)filtering, configuration [27-4](#)User Accounts panel, VPN wizard [33-11](#)

username

Clientless SSL VPN [38-1](#)Xauth for Easy VPN client [36-84](#)

---

**V**

version

ASDM [1-14](#)platform software [1-14](#)View/Config Banner [36-25](#)

virtual firewalls

See security contexts

Virtual Link panel [10-19](#)description [10-19](#)fields [10-19](#)

virtual MAC address

defining for Active/Active failover [13-31](#)

virtual MAC addresses

about [13-21, 13-32](#)defaults for Active/Active failover [13-31](#)defining [13-22](#)defining for Active/Standby failover [13-33](#)

virtual private network

overview [33-2](#)VLANs [6-3, 7-5](#)802.1Q trunk [6-3, 7-5](#)

ASA 5505

MAC addresses [8-4](#)maximum [8-2](#)subinterfaces [6-3, 7-5](#)**VoIP**proxy servers [25-20](#)**VPN**overview [33-1, 33-2](#)system options [36-80](#)VPN Client, IPSec attributes [35-9](#)VPN Tunnel Type panel, VPN wizard [33-2](#)VPN wizard [33-1](#)Address Pool panel [33-11](#)Address Translation Exemption panel [33-12](#)Attributes Pushed to Client panel [33-12](#)Client Authentication panel [33-9](#)IKE Policy panel [33-4](#)IPSec Encryption and Authentication panel [33-5](#)Remote Access Client panel [33-7](#)Remote Site Peer panel [33-3](#)Summary panel [33-7](#)User Accounts panel [33-11](#)VPN Tunnel Type panel [33-2](#)**VPNwizard**Local Hosts and Networks panel [33-6](#)New Authentication Server Group panel [33-10](#)VRRP [19-8](#)

## ***Beta Draft -- Cisco Confidential***

---

### **W**

web browsing with Clientless SSL VPN [38-4](#)

web clients, secure authentication [15-11](#)

Websense filtering server [27-1, 27-5](#)

WebVPN

    use suggestions [38-2](#)

Window menu [1-7](#)

Wizards menu [1-7](#)

---

### **X**

Xauth, Easy VPN client [36-84](#)

XDMCP

    application inspection, enabling [25-29](#)

---

### **Z**

Zone Labs Integrity Server [36-82](#)

***Beta Draft -- Cisco Confidential***