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

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

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

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

About This Guide xxii
   Document Objectives xxii
   Related Documentation xxii
   Document Conventions xxii
   Communications, Services, and Additional Information xxiii

CHAPTER 1

Introduction to Cisco ASA Firewall Services 1
   How to Implement Firewall Services 1
   Basic Access Control 2
   Application Filtering 2
   URL Filtering 3
   Threat Protection 3
   Firewall Services for Virtual Environments 4
   Network Address Translation 4
   Application Inspection 5
   Use Case: Expose a Server to the Public 5

PART I

Access Control 7

CHAPTER 2

Objects for Access Control 9
   Guidelines for Objects 9
   Configure Objects 10
      Configure Network Objects and Groups 10
      Configure a Network Object 10
      Configure a Network Object Group 11
      Configure Service Objects and Service Groups 12
CHAPTER 3

Access Control Lists  

About ACLs  

ACL Types  

ACL Names  

Access Control Entry Order  

Permit/Deny vs. Match/Do Not Match  

Access Control Implicit Deny  

IP Addresses Used for Extended ACLs When You Use NAT  

Time-Based ACEs  

Licensing for Access Control Lists  

Guidelines for ACLs  

Configure ACLs  

Basic ACL Configuration and Management Options  

Configure Extended ACLs  

Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching  

Add an Extended ACE for Port-Based Matching  

Add an Extended ACE for ICMP-Based Matching  

Add an Extended ACE for User-Based Matching (Identity Firewall)  

Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec)  

Examples for Extended ACLs  

Example of Converting Addresses to Objects for Extended ACLs  

Configure Standard ACLs  

Configure Webtype ACLs  

Add a Webtype ACE for URL Matching  

Add a Webtype ACE for IP Address Matching  

Examples for Webtype ACLs  

Configure a Service Object  

Configure a Service Group  

Configure Local User Groups  

Configure Security Group Object Groups  

Configure Time Ranges  

Monitoring Objects  

History for Objects  

CHAPTER 3

About ACLs  

ACL Types  

ACL Names  

Access Control Entry Order  

Permit/Deny vs. Match/Do Not Match  

Access Control Implicit Deny  

IP Addresses Used for Extended ACLs When You Use NAT  

Time-Based ACEs  

Licensing for Access Control Lists  

Guidelines for ACLs  

Configure ACLs  

Basic ACL Configuration and Management Options  

Configure Extended ACLs  

Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching  

Add an Extended ACE for Port-Based Matching  

Add an Extended ACE for ICMP-Based Matching  

Add an Extended ACE for User-Based Matching (Identity Firewall)  

Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec)  

Examples for Extended ACLs  

Example of Converting Addresses to Objects for Extended ACLs  

Configure Standard ACLs  

Configure Webtype ACLs  

Add a Webtype ACE for URL Matching  

Add a Webtype ACE for IP Address Matching  

Examples for Webtype ACLs
Access the ASA FirePOWER CLI 126
Configure ASA FirePOWER Basic Settings 126
Configure the ASA FirePOWER Module for ASDM Management 128
Configure the ASA FirePOWER Module 130
Configure the Security Policy on the ASA FirePOWER Module 130
Redirect Traffic to the ASA FirePOWER Module 130
Configure Inline or Inline Tap Monitor-Only Modes 130
Configure Passive Traffic Forwarding 132
Enable Captive Portal for Active Authentication 133
Managing the ASA FirePOWER Module 134
Install or Reimage the Module 134
    Install or Reimage the Software Module 134
    Reimage the 5585-X ASA FirePOWER Hardware Module 137
Reset the Password 139
Reload or Reset the Module 140
Shut Down the Module 140
Uninstall a Software Module Image 141
Session to the Software Module From the ASA 141
Upgrade the System Software 142
Monitoring the ASA FirePOWER Module 142
    Showing Module Status 143
    Showing Module Statistics 144
    Monitoring Module Connections 144
Examples for the ASA FirePOWER Module 145
History for the ASA FirePOWER Module 146

CHAPTER 8 149
Cisco Umbrella 149
    About Cisco Umbrella Connector 149
    Cisco Umbrella Enterprise Security Policy 149
    Cisco Umbrella Registration 150
Licensing Requirements for Cisco Umbrella Connector 150
Guidelines and Limitations for Cisco Umbrella 150
Configure Cisco Umbrella Connector 152
    Install the CA Certificate from the Cisco Umbrella Registration Server 153
Configure the Umbrella Connector Global Settings 155
Enable Umbrella in the DNS Inspection Policy Map 156
Verify the Umbrella Registration 157
Examples for the Umbrella Connector 158
  Example: Enabling Umbrella on the Global DNS Inspection Policy 158
  Example: Enabling Umbrella on an Interface with a Custom Inspection Policy 159
  Example: Enabling Both Umbrella and ASA FirePOWER 161
Monitoring the Umbrella Connector 162
  Monitoring the Umbrella Service Policy Statistics 162
  Monitoring Umbrella Syslog Messages 164
History for Cisco Umbrella Connector 164

CHAPTER 9

ASA and Cisco Cloud Web Security 165
  Information About Cisco Cloud Web Security 165
  User Identity and Cloud Web Security 166
  Authentication Keys 166
  ScanCenter Policy 166
    Directory Groups 167
    Custom Groups 167
      How Groups and the Authentication Key Interoperate 168
  Failover from Primary to Backup Proxy Server 168
Licensing Requirements for Cisco Cloud Web Security 169
Guidelines for Cloud Web Security 169
Configure Cisco Cloud Web Security 170
  Configure Communications with the Cloud Web Security Proxy Server 171
  Identify Whitelisted Traffic 173
  Configure a Service Policy to Send Traffic to Cloud Web Security 175
  Configure the User Identity Monitor 179
  Configure the Cloud Web Security Policy 179
Monitoring Cloud Web Security 180
Examples for Cisco Cloud Web Security 181
  Cloud Web Security Example with Identity Firewall 181
  Active Directory Integration Example for Identity Firewall 183
History for Cisco Cloud Web Security 186
Dynamic NAT 212
  About Dynamic NAT 212
    Dynamic NAT Disadvantages and Advantages 213
  Configure Dynamic Network Object NAT 214
  Configure Dynamic Twice NAT 216
Dynamic PAT 219
  About Dynamic PAT 219
    Dynamic PAT Disadvantages and Advantages 219
    PAT Pool Object Guidelines 220
  Configure Dynamic Network Object PAT 221
  Configure Dynamic Twice PAT 223
  Configure PAT with Port Block Allocation 226
  Configure Per-Session PAT or Multi-Session PAT 228
Static NAT 230
  About Static NAT 230
    Static NAT with Port Translation 230
    One-to-Many Static NAT 231
    Other Mapping Scenarios (Not Recommended) 232
  Configure Static Network Object NAT or Static NAT-with-Port-Translation 234
  Configure Static Twice NAT or Static NAT-with-Port-Translation 236
Identity NAT 239
  Configure Identity Network Object NAT 239
  Configure Identity Twice NAT 241
Monitoring NAT 243
History for NAT 244

CHAPTER 12

NAT Examples and Reference 249
Examples for Network Object NAT 249
  Providing Access to an Inside Web Server (Static NAT) 249
  NAT for Inside Hosts (Dynamic NAT) and NAT for an Outside Web Server (Static NAT) 250
  Inside Load Balancer with Multiple Mapped Addresses (Static NAT, One-to-Many) 252
  Single Address for FTP, HTTP, and SMTP (Static NAT-with-Port-Translation) 253
Examples for Twice NAT 254
  Different Translation Depending on the Destination (Dynamic Twice PAT) 254
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Components of a Service Policy</td>
<td>283</td>
</tr>
<tr>
<td>Features Configured with Service Policies</td>
<td>285</td>
</tr>
<tr>
<td>Feature Directionality</td>
<td>286</td>
</tr>
<tr>
<td>Feature Matching Within a Service Policy</td>
<td>287</td>
</tr>
<tr>
<td>Order in Which Multiple Feature Actions are Applied</td>
<td>288</td>
</tr>
<tr>
<td>Incompatibility of Certain Feature Actions</td>
<td>288</td>
</tr>
<tr>
<td>Feature Matching for Multiple Service Policies</td>
<td>289</td>
</tr>
<tr>
<td>Guidelines for Service Policies</td>
<td>290</td>
</tr>
<tr>
<td>Defaults for Service Policies</td>
<td>291</td>
</tr>
<tr>
<td>Default Service Policy Configuration</td>
<td>292</td>
</tr>
<tr>
<td>Default Class Maps (Traffic Classes)</td>
<td>293</td>
</tr>
<tr>
<td>Configure Service Policies</td>
<td>293</td>
</tr>
<tr>
<td>Identify Traffic (Layer 3/4 Class Maps)</td>
<td>295</td>
</tr>
<tr>
<td>Create a Layer 3/4 Class Map for Through Traffic</td>
<td>295</td>
</tr>
<tr>
<td>Create a Layer 3/4 Class Map for Management Traffic</td>
<td>298</td>
</tr>
<tr>
<td>Define Actions (Layer 3/4 Policy Map)</td>
<td>298</td>
</tr>
<tr>
<td>Apply Actions to an Interface (Service Policy)</td>
<td>300</td>
</tr>
<tr>
<td>Monitoring Service Policies</td>
<td>301</td>
</tr>
<tr>
<td>Examples for Service Policies (Modular Policy Framework)</td>
<td>301</td>
</tr>
<tr>
<td>Applying Inspection and QoS Policing to HTTP Traffic</td>
<td>301</td>
</tr>
<tr>
<td>Applying Inspection to HTTP Traffic Globally</td>
<td>302</td>
</tr>
<tr>
<td>Applying Inspection and Connection Limits to HTTP Traffic to Specific Servers</td>
<td>302</td>
</tr>
<tr>
<td>Applying Inspection to HTTP Traffic with NAT</td>
<td>303</td>
</tr>
<tr>
<td>History for Service Policies</td>
<td>304</td>
</tr>
<tr>
<td>CHAPTER 14</td>
<td></td>
</tr>
<tr>
<td>Getting Started with Application Layer Protocol Inspection</td>
<td>307</td>
</tr>
<tr>
<td>Application Layer Protocol Inspection</td>
<td>307</td>
</tr>
<tr>
<td>When to Use Application Protocol Inspection</td>
<td>307</td>
</tr>
<tr>
<td>Inspection Policy Maps</td>
<td>308</td>
</tr>
<tr>
<td>Replacing an In-Use Inspection Policy Map</td>
<td>308</td>
</tr>
<tr>
<td>How Multiple Traffic Classes are Handled</td>
<td>308</td>
</tr>
<tr>
<td>Guidelines for Application Inspection</td>
<td>309</td>
</tr>
<tr>
<td>Defaults for Application Inspection</td>
<td>311</td>
</tr>
<tr>
<td>Default Inspections and NAT Limitations</td>
<td>311</td>
</tr>
</tbody>
</table>
CHAPTER 15

Inspection of Basic Internet Protocols

DCERPC Inspection
  DCERPC Overview
  Configure a DCERPC Inspection Policy Map

DNS Inspection
  Defaults for DNS Inspection
  Configure DNS Inspection Policy Map

FTP Inspection
  FTP Inspection Overview
  Strict FTP
  Configure an FTP Inspection Policy Map

HTTP Inspection
  HTTP Inspection Overview
  Configure an HTTP Inspection Policy Map

ICMP Inspection
  ICMP Error Inspection

ILS Inspection
  Instant Messaging Inspection

IP Options Inspection
  Defaults for IP Options Inspection
  Configure an IP Options Inspection Policy Map

IPsec Pass Through Inspection
  IPsec Pass Through Inspection Overview
  Configure an IPsec Pass Through Inspection Policy Map

IPv6 Inspection
Configure a GTP Inspection Policy Map 401
Configure an SCTP Inspection Policy Map 405
Configure a Diameter Inspection Policy Map 406
Create a Custom Diameter Attribute-Value Pair (AVP) 410
Inspecting Encrypted Diameter Sessions 411
  Configure Server Trust Relationship with Diameter Clients 413
  Configure Full TLS Proxy with Static Client Certificate for Diameter Inspection 414
  Configure Full TLS Proxy with Local Dynamic Certificates for Diameter Inspection 417
  Configure TLS Proxy with TLS Offload for Diameter Inspection 421
Configure an M3UA Inspection Policy Map 422
Configure the Mobile Network Inspection Service Policy 425
Configure RADIUS Accounting Inspection 427
  Configure a RADIUS Accounting Inspection Policy Map 427
  Configure the RADIUS Accounting Inspection Service Policy 429
Monitoring Mobile Network Inspection 430
  Monitoring GTP Inspection 430
  Monitoring SCTP 431
  Monitoring Diameter 432
  Monitoring M3UA 433
History for Mobile Network Inspection 434

PART V

Connection Management and Threat Detection 437

CHAPTER 18

Connection Settings 439
  What Are Connection Settings? 439
  Configure Connection Settings 440
    Configure Global Timeouts 441
    Protect Servers from a SYN Flood DoS Attack (TCP Intercept) 443
    Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer) 445
    Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass) 449
      The Asynchronous Routing Problem 449
      Guidelines and Limitations for TCP State Bypass 450
    Configure TCP State Bypass 451
    Disable TCP Sequence Randomization 452
### CHAPTER 19: Quality of Service

- **About QoS** 465
  - Supported QoS Features 465
  - What is a Token Bucket? 466
  - Policing 466
  - Priority Queuing 466
  - How QoS Features Interact 467
  - DSCP (DiffServ) Preservation 467
- **Guidelines for QoS** 467
- **Configure QoS** 468
  - Determine the Queue and TX Ring Limits for a Priority Queue 468
    - Queue Limit Worksheet 468
    - TX Ring Limit Worksheet 469
  - Configure the Priority Queue for an Interface 469
  - Configure a Service Rule for Priority Queuing and Policing 471
- **Monitor QoS** 473
  - QoS Police Statistics 473
  - QoS Priority Statistics 474
  - QoS Priority Queue Statistics 474
- **Configuration Examples for Priority Queuing and Policing** 475
  - Class Map Examples for VPN Traffic 475
  - Priority and Policing Example 476
- **History for QoS** 477

### CHAPTER 20: Threat Detection

- **Detecting Threats** 479
  - Basic Threat Detection Statistics 480
Advanced Threat Detection Statistics  480
Scanning Threat Detection  481
Guidelines for Threat Detection  481
Defaults for Threat Detection  482
Configure Threat Detection  483
   Configure Basic Threat Detection Statistics  483
   Configure Advanced Threat Detection Statistics  484
   Configure Scanning Threat Detection  485
Monitoring Threat Detection  486
   Monitoring Basic Threat Detection Statistics  486
   Monitoring Advanced Threat Detection Statistics  487
   Evaluating Host Threat Detection Statistics  489
   Monitoring Shunned Hosts, Attackers, and Targets  491
Examples for Threat Detection  492
History for Threat Detection  493
About This Guide

The following topics explain how to use this guide.

- Document Objectives, on page xxi
- Related Documentation, on page xxi
- Document Conventions, on page xxi
- Communications, Services, and Additional Information, on page xxiii

Document Objectives

The purpose of this guide is to help you configure the firewall features for the Cisco ASA series using the command-line interface. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can also configure and monitor the ASA by using the Adaptive Security Device Manager (ASDM), a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online help for less common scenarios.

Throughout this guide, the term “ASA” applies generically to supported models, unless specified otherwise.

Related Documentation

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

Document Conventions

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

<table>
<thead>
<tr>
<th>Text Conventions</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Commands, keywords, button labels, field names, and user-entered text appear in <strong>boldface</strong>. For menu-based commands, the full path to the command is shown.</td>
</tr>
</tbody>
</table>
### Convention | Indication
--- | ---
italic | Variables, for which you supply values, are presented in an *italic* typeface. Italics are also used for document titles, and for general emphasis.

monospace | Terminal sessions and information that the system displays appear in monospace type.

{x | y | z} | Required alternative keywords are grouped in braces and separated by vertical bars.

[] | Elements in square brackets are optional.

[x | y | z] | Optional alternative keywords are grouped in square brackets and separated by vertical bars.

[] | Default responses to system prompts are also in square brackets.

<> | Non-printing characters such as passwords are in angle brackets.

! | An exclamation point (!) or a number sign (#) at the beginning of a line of code indicates a comment line.

---

### Reader Alerts

This document uses the following for reader alerts:

<table>
<thead>
<tr>
<th>Reader Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>reader take note. Notes contain helpful suggestions or references to material not covered in the manual.</td>
</tr>
<tr>
<td>Tip</td>
<td>the following information will help you solve a problem.</td>
</tr>
<tr>
<td>Caution</td>
<td>reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.</td>
</tr>
<tr>
<td>Timesaver</td>
<td>the described action saves time. You can save time by performing the action described in the paragraph.</td>
</tr>
<tr>
<td>Warning</td>
<td>reader be warned. In this situation, you might perform an action that could result in bodily injury.</td>
</tr>
</tbody>
</table>
Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Firewall services are those ASA features that are focused on controlling access to the network, including services that block traffic and services that enable traffic flow between internal and external networks. These services include those that protect the network against threats, such as Denial of Service (DoS) and other attacks.

The following topics provide an overview of firewall services.

- How to Implement Firewall Services, on page 1
- Basic Access Control, on page 2
- Application Filtering, on page 2
- URL Filtering, on page 3
- Threat Protection, on page 3
- Firewall Services for Virtual Environments, on page 4
- Network Address Translation, on page 4
- Application Inspection, on page 5
- Use Case: Expose a Server to the Public, on page 5

How to Implement Firewall Services

The following procedure provides a general sequence for implementing firewall services. However, each step is optional, needed only if you want to provide the service to your network.

Before you begin

Configure the ASA according to the general operations configuration guide, including at minimum basic settings, interface configuration, routing, and management access.

Procedure

Step 1 Implement access control for the network. See Basic Access Control, on page 2.
Step 2 Implement application filtering. See Application Filtering, on page 2.
Step 3 Implement URL filtering. See URL Filtering, on page 3.
**Basic Access Control**

Access rules, applied per interface or globally, are your first line of defense. You can drop, upon entry, specific types of traffic, or traffic from (or to) specific hosts or networks. By default, the ASA allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level).

You can apply an access rule to limit traffic from inside to outside, or allow traffic from outside to inside.

Basic access rules control traffic using a “5-tuple” of source address and port, destination address and port, and protocol. See Access Rules, on page 45 and Access Control Lists, on page 21.

You can augment your rules by making them identity aware. This lets you configure rules based on user identity or group membership. To implement identity control, do any combination of the following:

- Install Cisco Context Directory Agent (CDA), also known as AD agent, on a separate server to collect user and group information already defined in your Active Directory (AD) server. Then, configure the ASA to get this information, and add user or group criteria to your access rules. See Identity Firewall, on page 61.

- Install Cisco Identity Services Engine (ISE) on a separate server to implement Cisco Trustsec. You can then add security group criteria to your access rules. See ASA and Cisco TrustSec, on page 85.

- Install the ASA FirePOWER module on the ASA and implement identity policies in the module. The identity-aware access policies in ASA FirePOWER would apply to any traffic that you redirect to the module. See ASA FirePOWER Module, on page 115.

**Application Filtering**

The wide-spread use of web-based applications means that a lot of traffic runs over the HTTP or HTTPS protocols. With traditional 5-tuple access rules, you either allow or disallow all HTTP/HTTPS traffic. You might require more granular control of web traffic.

You can install a module on the ASA to provide application filtering to selectively allow HTTP or other traffic based on the application being used. Thus, you do not have to make a blanket permit for HTTP. You can look inside the traffic and prevent applications that are unacceptable for your network (for example, inappropriate file sharing). When you add a module for application filtering, do not configure HTTP inspection on the ASA.

To implement application filtering, install the ASA FirePOWER module on the ASA and use application filtering criteria in your ASA FirePOWER access rules. These policies apply to any traffic that you redirect to the module. See ASA FirePOWER Module, on page 115.
URL Filtering

URL filtering denies or allows traffic based on the URL of the destination site.

The purpose of URL filtering is primarily to completely block or allow access to a web site. Although you can target individual pages, you typically specify a host name (such as www.example.com) or a URL category, which defines a list of host names that provide a particular type of service (such as Gambling).

When trying to decide whether to use URL filtering or application filtering for HTTP/HTTPS traffic, consider whether your intention is to create a policy that applies to all traffic directed at a web site. If your intention is to treat all such traffic the same way (denying it or allowing it), use URL filtering. If your intention is to selectively block or allow traffic to the site, use application filtering.

To implement URL filtering, do one of the following:

• Install the ASA FirePOWER module on the ASA and use URL filtering criteria in your ASA FirePOWER access rules. These policies apply to any traffic that you redirect to the module. See ASA FirePOWER Module, on page 115.

• Subscribe to the Cisco Umbrella service, where you configure the Enterprise Security policy to block malicious sites based on the fully-qualified domain name (FQDN). For FQDNs that are considered suspicious, you can redirect user connections to the Cisco Umbrella intelligent proxy, which performs URL filtering. The Umbrella service works by handling users' DNS lookup requests, returning the IP address for a block page or the IP address of the intelligent proxy. The service returns the real IP address for an FQDN for whitelisted domains. See Cisco Umbrella, on page 149.

• Subscribe to the Cloud Web Security service, where you configure your filtering policies in ScanCenter, and then configure the ASA to send traffic to your Cloud Web Security account. See ASA and Cisco Cloud Web Security, on page 165.

Threat Protection

You can implement a number of measures to protect against scanning, denial of service (DoS), and other attacks. A number of ASA features help protect against attacks by applying connection limits and dropping abnormal TCP packets. Some features are automatic, others are configurable but have defaults appropriate in most cases, while others are completely optional and you must configure them if you want them.

Following are the threat protection services available with the ASA.

• IP packet fragmentation protection—The ASA performs full reassembly of all ICMP error messages and virtual reassembly of the remaining IP fragments that are routed through the ASA, and drops fragments that fail the security check. No configuration is necessary.

• Connection limits, TCP normalization, and other connection-related features—Configure connection-related services such as TCP and UDP connection limits and timeouts, TCP sequence number randomization, TCP normalization, and TCP state bypass. TCP normalization is designed to drop packets that do not appear normal. See Connection Settings, on page 439.

For example, you can limit TCP and UDP connections and embryonic connections (a connection request that has not finished the necessary handshake between source and destination). Limiting the number of connections and embryonic connections protects you from a DoS attack. The ASA 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.

- Threat detection—Implement threat detection on the ASA to collect statistics to help identify attacks. Basic threat detection is enabled by default, but you can implement advanced statistics and scanning threat detection. You can shun hosts that are identified as a scanning threat. See Threat Detection, on page 479.

- Next-Generation IPS—Install the ASA FirePOWER module on the ASA and implement Next Generation IPS intrusion rules in your ASA FirePOWER. These policies would apply to any traffic that you redirect to ASA FirePOWER. See ASA FirePOWER Module, on page 115.

Firewall Services for Virtual Environments

Virtual environments deploy servers as virtual machines, for example, in VMware ESXi. The firewalls in a virtual environment can be traditional hardware devices, or they can also be virtual machine firewalls, such as the ASAv.

Traditional and next-generation firewall services apply to virtual environments in the same way that they apply to environments that do not use virtual machine servers. However, virtual environments can provide additional challenges, because it is easy to create and tear down servers.

Additionally, traffic between servers within the data center might require as much protection as traffic between the data center and external users. For example, if an attacker gains control of a server within the data center, that could open up attacks on other servers in the data center.

Firewall services for virtual environments add capabilities to apply firewall protection specifically to virtual machines. Following are the firewall services available for virtual environments:

- Attribute-based access control—You can configure network objects to match traffic based on attributes, and use those objects in access control rules. This lets you decouple firewall rules from network topology. For example, you can allow all hosts with the Engineering attribute to access hosts with the Lab Server attribute. You could then add/remove hosts with these attributes and the firewall policy would be applied automatically without the need for updating access rules. For more information, see Attribute-Based Access Control, on page 189.

Network Address Translation

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because you can advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security—Keeping internal IP addresses hidden discourages direct attacks.

- IP routing solutions—Overlapping IP addresses are not a problem when you use NAT.
• Flexibility—You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.

• Translating between IPv4 and IPv6 (Routed mode only)—If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

NAT is not required. If you do not configure NAT for a given set of traffic, that traffic will not be translated, but will have all of the security policies applied as normal.

See:

• Network Address Translation (NAT), on page 201
• NAT Examples and Reference, on page 249

Application Inspection

Application 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 ASA to do a deep packet inspection, to open the required pinholes and to apply network address translation (NAT).

The default ASA policy already applies inspection globally for many popular protocols, such as DNS, FTP, SIP, ESMTP, TFTP, and others. The default inspections might be all you require for your network.

However, you might need to enable inspection for other protocols, or fine-tune an inspection. Many inspections include detailed options that let you control packets based on their contents. If you know a protocol well, you can apply fine-grained control on that traffic.

You use service policies to configure application inspection. You can configure a global service policy, or apply a service policy to each interface, or both.

See:

• Service Policy, on page 283
• Getting Started with Application Layer Protocol Inspection, on page 307
• Inspection of Basic Internet Protocols, on page 329
• Inspection for Voice and Video Protocols, on page 369
• Inspection for Mobile Networks, on page 393.

Use Case: Expose a Server to the Public

You can make certain application services on a server available to the public. For example, you could expose a web server, so that users can connect to the web pages but not make any other connections to the server.

To expose a server to the public, you typically need to create access rules that allow the connection and NAT rules to translate between the server’s internal IP address and an external address that the public can use. In addition, you can use port address translation (PAT) to map an internal port to an external port, if you do not want the externally exposed service to use the same port as the internal server. For example, if the internal web server is not running on TCP/80, you can map it to TCP/80 to make connections easier for external users.
The following example makes a web server on the inside private network available for public access.

**Figure 1: Static NAT for an Inside Web Server**

![Diagram showing how to set up static NAT for an inside web server](image)

**Procedure**

**Step 1**  
Create a network object for the internal web server.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

**Step 2**  
Configure static NAT for the object:

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

**Step 3**  
Add an access rule to the access group attached to the outside interface to permit web access to the server.

```
hostname(config)# access-list outside_access_in line 1 extended
permit tcp any4 object myWebServ eq http
```

**Step 4**  
If you do not already have an access group on the outside interface, apply it using the access-group command:

```
hostname(config)# access-group outside_access_in in interface outside
```
PART I

Access Control

• Objects for Access Control, on page 9
• Access Control Lists, on page 21
• Access Rules, on page 45
• Identity Firewall, on page 61
• ASA and Cisco TrustSec, on page 85
• ASA FirePOWER Module, on page 115
• Cisco Umbrella, on page 149
• ASA and Cisco Cloud Web Security, on page 165
Objects for Access Control

Objects are reusable components for use in your configuration. You can define and use them in Cisco ASA configurations in the place of inline IP addresses, services, names, and so on. Objects make it easy to maintain your configurations because you can modify an object in one place and have it be reflected in all other places that are referencing it. Without objects you would have to modify the parameters for every feature when required, instead of just once. For example, if a network object defines an IP address and subnet mask, and you want to change the address, you only need to change it in the object definition, not in every feature that refers to that IP address.

- Guidelines for Objects, on page 9
- Configure Objects, on page 10
- Monitoring Objects, on page 18
- History for Objects, on page 19

Guidelines for Objects

IPv6 Guidelines

Supports IPv6 with the following restrictions:

- You can mix IPv4 and IPv6 entries in a network object group, but you cannot use a mixed object group for NAT.

Additional Guidelines and Limitations

- Objects must have unique names, because objects and object groups share the same name space. While you might want to create a network object group named “Engineering” and a service object group named “Engineering,” you need to add an identifier (or “tag”) to the end of at least one object group name to make it unique. For example, you can use the names “Engineering_admins” and “Engineering_hosts” to make the object group names unique and to aid in identification.

- Object names are limited to 64 characters, including letters, numbers, and these characters: !@#$%^&()-_. Object names are case-sensitive.

- You cannot remove an object or make an object empty if it is used in a command, unless you enable forward referencing (the forward-reference enable command).
Configure Objects

The following sections describe how to configure objects that are primarily used on access control.

Configure Network Objects and Groups

Network objects and groups identify IP addresses or host names. Use these objects in access control lists to simplify your rules.

Configure a Network Object

A network object can contain a host, a network IP address, a range of IP addresses, or a fully qualified domain name (FQDN).

You can also enable NAT rules on the object (excepting FQDN objects). For more information about configuring object NAT, see Network Address Translation (NAT), on page 201.

Procedure

Step 1 Create or edit a network object using the object name: `object network object_name`

Example:

hostname(config)# object network email-server

Step 2 Add an address to the object using one of the following commands. Use the `no` form of the command to remove the object.

- **host** `{IPv4_address | IPv6_address}`—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8:0DB8:800:200C:417A.

- **subnet** `{IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}`—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

- **range** `start_address end_address`—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

- **fqdn** `{v4 | v6} fully_qualified_domain_name`—A fully-qualified domain name, that is, the name of a host, such as www.example.com. Specify `v4` to limit the address to IPv4, and `v6` for IPv6. If you do not specify an address type, IPv4 is assumed.

Example:

hostname(config-network-object)# host 10.2.2.2

Step 3 (Optional) Add a description: `description string`
Configure a Network Object Group

Network object groups can contain multiple network objects as well as inline networks or hosts. Network object groups can include a mix of both IPv4 and IPv6 addresses.

However, you cannot use a mixed IPv4 and IPv6 object group for NAT, or object groups that include FQDN objects.

Procedure

Step 1
Create or edit a network object group using the object name: **object-group network** group_name

Example:

```
hostname(config)# object-group network admin
```

Step 2
Add objects and addresses to the network object group using one or more of the following commands. Use the **no** form of the command to remove an object.

- **network-object host** [IPv4_address | IPv6_address] — The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.

- **network-object** [IPv4_address IPv4_mask | IPv6_address | IPv6_prefix] — The address of a network or host. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

- **network-object object** object_name — The name of an existing network object.

- **group-object** object_group_name — The name of an existing network object group.

Example:

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8::0dB8:800:200C:417A
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# group-object existing-network-object-group
```

Step 3
(Optional) Add a description: **description** string

Examples

To create a network group that includes the IP addresses of three administrators, enter the following commands:

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```
Create network object groups for privileged users from various departments by entering the following commands:

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

You then nest all three groups together as follows:

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

**Configure Service Objects and Service Groups**

Service objects and groups identify protocols and ports. Use these objects in access control lists to simplify your rules.

**Configure a Service Object**

A service object can contain a single protocol specification.

**Procedure**

**Step 1** Create or edit a service object using the object name: `object service object_name`

**Example:**

```
hostname(config)# object service web
```

**Step 2** Add a service to the object using one of the following commands. Use the `no` form of the command to remove an object.

- `service protocol`—The name or number (0-255) of an IP protocol. Specify `ip` to apply to all protocols.

- `service {icmp | icmp6} [icmp-type [icmp_code]]`—For ICMP or ICMP version 6 messages. You can optionally specify the ICMP type by name or number (0-255) to limit the object to that message type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used.
You can optionally specify ports for the source, destination, or both. You can specify the port by name or number. The operator can be one of the following:

- `lt`—less than.
- `gt`—greater than.
- `eq`—equal to.
- `neq`—not equal to.
- `range`—an inclusive range of values. When you use this operator, specify two port numbers, for example, `range 100 200`.

Example:

```
hostname(config-service-object)# service tcp destination eq http
```

### Configure a Service Group

A service object group includes a mix of protocols, if desired, including optional source and destination ports for protocols that use them, and ICMP type and code.

#### Before you begin

You can model all services using the generic service object group, which is explained here. However, you can still configure the types of service group objects that were available prior to ASA 8.3(1). These legacy objects include TCP/UDP/TCP-UDP port groups, protocol groups, and ICMP groups. The contents of these groups are equivalent to the associated configuration in the generic service object group, with the exception of ICMP groups, which do not support ICMP6 or ICMP codes. If you still want to use these legacy objects, for detailed instructions, see the `object-service` command description in the command reference on Cisco.com.

#### Procedure

**Step 1**
Create or edit a service object group using the object name: `object-group service object_name`

Example:

```
hostname(config)# object-group service general-services
```

**Step 2**
Add objects and services to the service object group using one or more of the following commands. Use the `no` form of the command to remove an object.

- `service-object protocol`—The name or number (0-255) of an IP protocol. Specify `ip` to apply to all protocols.

- `service-object {icmp | icmp6} [icmp-type [icmp_code]]`—For ICMP or ICMP version 6 messages. You can optionally specify the ICMP type by name or number (0-255) to limit the object to that message.
Configure a Service Group

Access Control

Configure a Service Group

Step 3 (Optional) Add a description: description string

Examples

The following example shows how to add both TCP and UDP services to a service object group:

hostname(config)# object-group service CommonApps
hostname(config)# service-object tcp destination eq ftp
hostname(config)# service-object tcp-udp destination eq www
hostname(config)# service-object tcp destination eq h323
hostname(config)# service-object tcp destination eq https
hostname(config)# service-object udp destination eq ntp

The following example shows how to add multiple service objects to a service object group:

hostname(config)# object service SSH
hostname(config)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config)# service eigrp
hostname(config)# object service HTTPS
hostname(config)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config)# service-object object SSH
hostname(config)# service-object object EIGRP

type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used.

• service-object \{tcp | udp | tcp-udp | sctp\} \{source operator port\} \{destination operator port\}—For TCP, UDP, or both, or for SCTP. You can optionally specify ports for the source, destination, or both. You can specify the port by name or number. The operator can be one of the following:

  • lt—less than.
  • gt—greater than.
  • eq—equal to.
  • neq—not equal to.
  • range—an inclusive range of values. When you use this operator, specify two port numbers, for example, range 100 200.

• service-object object object_name—The name of an existing service object.

• group-object object object_group_name—The name of an existing service object group.

Example:

hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
Configure Local User Groups

You can create local user groups for use in features that support the identity firewall by including the group in an extended ACL, which in turn can be used in an access rule, for example.

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for identity-based rules. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups.

A user can belong to local user groups and user groups imported from Active Directory.

Because you can use usernames and user group names directly in an ACL, you need to configure local user groups only if:

- You want to create a group of users defined in the LOCAL database.
- You want to create a group of users or user groups that are not captured in a single user group defined on the AD server.

**Procedure**

**Step 1**
Create or edit a user object group using the object name: `object-group user group_name`

**Example:**

```
hostname(config)# object-group user admins
```

**Step 2**
Add users and groups to the user object group using one or more of the following commands. Use the `no` form of the command to remove an object.

- `user [domain_NETBIOS_name]username`—A username. If there is a space in the domain name or username, you must enclose the domain name and user name in quotation marks. The domain name can be LOCAL (for users defined in the local database) or an Active Directory (AD) domain name as specified in the `user-identity domain domain_NetBIOS_name aaa-server aaa_server_group_tag` command.
  
  When adding users defined in an AD domain, the `user_name` must be the Active Directory sAMAccountName, which is unique, instead of the common name (cn), which might not be unique. If you do not specify a domain name, the default is used, which is either LOCAL or the one defined on the `user-identity default-domain` command.

- `user-group [domain_NETBIOS_name\\]username`—A user group. If there is a space in the domain name or group name, you must enclose the domain name and group name in quotation marks. Note the double `\` that separates the domain and group names.

- `group-object object_group_name`—The name of an existing user object group.

**Example:**
Configure Security Group Object Groups

You can create security group object groups for use in features that support Cisco TrustSec by including the group in an extended ACL, which in turn can be used in an access rule, for example.

When integrated with Cisco TrustSec, the ASA downloads security group information from the ISE. The ISE acts as an identity repository, by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping. You provision and manage security group ACLs centrally on the ISE.

However, the ASA might have localized network resources that are not defined globally that require local security groups with localized security policies. Local security groups can contain nested security groups that are downloaded from the ISE. The ASA consolidates local and central security groups.

To create local security groups on the ASA, you create a local security object group. A local security object group can contain one or more nested security object groups or Security IDs or security group names. You can also create a new Security ID or security group name that does not exist on the ASA.

You can use the security object groups you create on the ASA to control access to network resources. You can use the security object group as part of an access group or service policy.

Tip

If you create a group with tags or names that are not known to the ASA, any rules that use the group will be inactive until the tags or names are resolved with ISE.

Procedure

Step 1

Create or edit a security group object group using the object name: `object-group security group_name`

Example:

```
hostname(config)# object-group security mktg-sg
```

Step 2

Add objects to the service group object group using one or more of the following commands. Use the `no` form of the command to remove an object.

- `security-group {tag sgt_number | name sg_name}`—A security group tag (SGT) or name. A tag is a number from 1 to 65533 and is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB) by the ISE. Security group names are created on the ISE and provide user-friendly names for security groups. The security group table maps SGTs to security group names. Consult your ISE configuration for the valid tags and names.

- `group-object object_group_name`—The name of an existing security group object group.
Configure Time Ranges

A time range object defines a specific time consisting of a start time, an end time, and optional recurring entries. You use these objects on ACL rules to provide time-based access to certain features or assets. For example, you could create an access rule that allows access to a particular server during working hours only.

You can include multiple periodic entries in a time range object. If a time range has both absolute and periodic values specified, then the periodic values are evaluated only after the absolute start time is reached, and they are not further evaluated after the absolute end time is reached.

Creating a time range does not restrict access to the device. This procedure defines the time range only. You must then use the object in an access control rule.

Procedure

Step 1
Create the time range: `time-range name`

Step 2
(Optional.) Add a start or end time (or both) to the time range.

`absolute [start time date] [end time date]`

If you do not specify a start time, the default start time is now.

The `time` is in the 24-hour format `hh:mm`. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

The `date` is in the format `day month year`; for example, `1 January 2014`.

Step 3
(Optional.) Add recurring time periods.

`periodic days-of-the-week time to [days-of-the-week] time`

You can specify the following values for `days-of-the-week`. Note that you can specify a second day of the week only if you specify a single day for the first argument.

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday. You can specify more than one of these, separated by spaces, for the first `days-of-the-week` argument.
- daily
- weekdays
- weekend

The `time` is in the 24-hour format `hh:mm`. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
Monitoring Objects

To monitor objects and groups, enter the following commands:

- **show access-list**
  
  Displays the access list entries. Entries that include objects are also expanded out into individual entries based on the object contents.

- **show running-config object [id object_id]**
  
  Displays all current objects. Use the id keyword to view a single object by name.

- **show running-config object object_type**
  
  Displays the current objects by their type, network or service.

- **show running-config object-group [id group_id]**
  
  Displays all current object groups. Use the id keyword to view a single object group by name.

- **show running-config object-group grp_type**
  
  Displays the current object groups by their group type.
## History for Objects

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object groups</td>
<td>7.0(1)</td>
<td>Object groups simplify ACL creation and maintenance. We introduced or modified the following commands: object-group protocol, object-group network, object-group service, object-group icmp_type.</td>
</tr>
<tr>
<td>Regular expressions and policy maps</td>
<td>7.2(1)</td>
<td>Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: class-map type regex, regex, match regex.</td>
</tr>
<tr>
<td>Objects</td>
<td>8.3(1)</td>
<td>Object support was introduced. We introduced or modified the following commands: object-network, object-service, object-group network, object-group service, network object, access-list extended, access-list webtype, access-list remark.</td>
</tr>
<tr>
<td>User Object Groups for Identity Firewall</td>
<td>8.4(2)</td>
<td>User object groups for identity firewall were introduced. We introduced the following commands: object-network user, user.</td>
</tr>
<tr>
<td>Security Group Object Groups for Cisco TrustSec</td>
<td>8.4(2)</td>
<td>Security group object groups for Cisco TrustSec were introduced. We introduced the following commands: object-network security, security.</td>
</tr>
<tr>
<td>Mixed IPv4 and IPv6 network object groups</td>
<td>9.0(1)</td>
<td>Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses. <strong>Note</strong> You cannot use a mixed object group for NAT. We modified the following commands: object-group network.</td>
</tr>
<tr>
<td>Extended ACL and object enhancement to filter ICMP traffic by ICMP code</td>
<td>9.0(1)</td>
<td>ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: access-list extended, service-object, service.</td>
</tr>
<tr>
<td>Service object support for Stream Control Transmission Protocol (SCTP)</td>
<td>9.5(2)</td>
<td>You can now create service objects and groups that specific SCTP ports. We modified the following commands: service-object, service.</td>
</tr>
</tbody>
</table>
CHAPTER 3

Access Control Lists

Access control lists (ACLs) are used by many different features. When applied to interfaces or globally as access rules, they permit or deny traffic that flows through the appliance. For other features, the ACL selects the traffic to which the feature will apply, performing a matching service rather than a control service.

The following sections explain the basics of ACLs and how to configure and monitor them. Access rules, ACLs applied globally or to interfaces, are explained in more detail in Access Rules, on page 45.

- About ACLs, on page 21
- Licensing for Access Control Lists, on page 25
- Guidelines for ACLs, on page 25
- Configure ACLs, on page 26
- Edit ACLs in an Isolated Configuration Session, on page 40
- Monitoring ACLs, on page 42
- History for ACLs, on page 42

About ACLs

Access control lists (ACLs) identify traffic flows by one or more characteristics, including source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the type of ACL. ACLs are used in a variety of features. ACLs are made up of one or more access control entries (ACEs).

ACL Types

The ASA uses the following types of ACLs:

- Extended ACLs—Extended ACLs are the main type that you will use. These ACLs are used for access rules to permit and deny traffic through the device, and for traffic matching by many features, including service policies, AAA rules, WCCP, Botnet Traffic Filter, and VPN group and DAP policies. See Configure Extended ACLs, on page 28.

- EtherType ACLs—EtherType ACLs apply to non-IP layer-2 traffic on bridge group member interfaces only. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet. With EtherType ACLs, you can control the flow of non-IP traffic across the device. See Configure EtherType ACLs, on page 39.

- Webtype ACLs—Webtype ACLs are used for filtering clientless SSL VPN traffic. These ACLs can deny access based on URLs or destination addresses. See Configure Webtype ACLs, on page 35.
• Standard ACLs—Standard ACLs identify traffic by destination address only. There are few features that use them: route maps and VPN filters. Because VPN filters also allow extended access lists, limit standard ACL use to route maps. See Configure Standard ACLs, on page 34.

The following table lists some common uses for ACLs and the type to use.

### Table 1: ACL Types and Common Uses

<table>
<thead>
<tr>
<th>ACL Use</th>
<th>ACL Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control network access for IP traffic (routed and transparent mode)</td>
<td>Extended</td>
<td>The ASA does not allow any traffic from a lower security interface to a higher security interface unless it is explicitly permitted by an extended ACL. In routed mode, you must use an ACL to permit traffic between a bridge group member interface and an interface outside same the bridge group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> To access the ASA interface for management access, you do not also need an ACL allowing the host IP address. You only need to configure management access according to the general operations configuration guide.</td>
</tr>
<tr>
<td>Identify traffic for AAA rules</td>
<td>Extended</td>
<td>AAA rules use ACLs to identify traffic.</td>
</tr>
<tr>
<td>Augment network access control for IP traffic for a given user</td>
<td>Extended, downloaded from a AAA server per user</td>
<td>You can configure the RADIUS server to download a dynamic ACL to be applied to the user, or the server can send the name of an ACL that you already configured on the ASA.</td>
</tr>
<tr>
<td>VPN access and filtering</td>
<td>Extended, Standard</td>
<td>Group policies for remote access and site to site VPNs use standard or extended ACLs for filtering. Remote access VPNs also use extended ACLs for client firewall configurations and dynamic access policies.</td>
</tr>
<tr>
<td>Identify traffic in a traffic class map for Modular Policy Framework</td>
<td>Extended</td>
<td>ACLs can be used to identify traffic in a class map, which is used for features that support Modular Policy Framework. Features that support Modular Policy Framework include TCP and general connection settings, and inspection.</td>
</tr>
<tr>
<td>For bridge group member interfaces, control network access for non-IP traffic</td>
<td>EtherType</td>
<td>You can configure an ACL that controls traffic based on its EtherType for any interface that is a member of a bridge group.</td>
</tr>
<tr>
<td>Identify route filtering and redistribution</td>
<td>Standard, Extended</td>
<td>Various routing protocols use standard ACLs for route filtering and redistribution (through route maps) for IPv4 addresses, and extended ACLs for IPv6.</td>
</tr>
<tr>
<td>Filtering for clientless SSL VPN</td>
<td>Webtype</td>
<td>You can configure a webtype ACL to filter URLs and destinations.</td>
</tr>
</tbody>
</table>
ACL Names

Each ACL has a name or numeric ID, such as outside_in, OUTSIDE_IN, or 101. Limit the names to 241 characters or fewer. Consider using all uppercase letters to make it easier to find the name when viewing a running configuration.

Develop a naming convention that will help you identify the intended purpose of the ACL. For example, ASDM uses the convention interface-name_purpose_direction, such as “outside_access_in”, for an ACL applied to the “outside” interface in the inbound direction.

Traditionally, ACL IDs were numbers. Standard ACLs were in the range 1-99 or 1300-1999. Extended ACLs were in the range 100-199 or 2000-2699. The ASA does not enforce these ranges, but if you want to use numbers, you might want to stick to these conventions to maintain consistency with routers running IOS Software.

Access Control Entry Order

An ACL is made up of one or more ACEs. Unless you explicitly insert an ACE at a given line, each ACE that you enter for a given ACL name is appended to the end of the ACL.

The order of ACEs is important. When the ASA decides whether to forward or drop a packet, the ASA 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.

Thus, if you place a more specific rule after a more general rule, the more specific rule might never be hit. For example, if you want to permit network 10.1.1.0/24, but drop traffic from host 10.1.1.15 on that subnet, the ACE that denies 10.1.1.15 must come before the one that permits 10.1.1.0/24. If the permit 10.1.1.0/24 ACE comes first, 10.1.1.15 will be allowed, and the deny ACE will never be matched.

In an extended ACL, use the line number parameter on the access-list command to insert rules at the right location. Use the show access-list name command to view the ACL entries and their line numbers to help determine the right number to use. For other types of ACL, you must rebuild the ACL (or better, use ASDM) to change the order of ACEs.

Permit/Deny vs. Match/Do Not Match

Access control entries either “permit” or “deny” traffic that matches the rule. When you apply an ACL to a feature that determines whether traffic is allowed through the ASA or is dropped, such as global and interface access rules, “permit” and “deny” mean what they say.

For other features, such as service policy rules, “permit” and “deny” actually mean “match” or “do not match.” In these cases, the ACL is selecting the traffic that should receive the services of that feature, such as application inspection or redirection to a service module. “Denied” traffic is simply traffic that does not match the ACL, and thus will not receive the service.

Access Control Implicit Deny

ACLs that are used for through-the-box access rules have an implicit deny statement at the end. Thus, for traffic controlling ACLs such as those applied to interfaces, if you do not explicitly permit a type of traffic, that traffic is dropped. For example, if you want to allow all users to access a network through the ASA except for one or more particular addresses, then you need to deny those particular addresses and then permit all others.
For management (control plane) ACLs, which control to-the-box traffic, there is no implicit deny at the end of a set of management rules for an interface. Instead, any connection that does not match a management access rule is then evaluated by regular access control rules.

For ACLs used to select traffic for a service, you must explicitly “permit” the traffic; any traffic not “permitted” will not be matched for the service; “denied” traffic bypasses the service.

For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (or implicitly allowed from a high security interface to a low security interface). However, if you explicitly deny all traffic with an EtherType ACE, then IP and ARP traffic is denied; only physical protocol traffic, such as auto-negotiation, is still allowed.

**IP Addresses Used for Extended ACLs When You Use NAT**

When you use NAT or PAT, you are translating addresses or ports, typically mapping between internal and external addresses. If you need to create an extended ACL that applies to addresses or ports that have been translated, you need to determine whether to use the real (untranslated) addresses or ports or the mapped ones. The requirement differs by feature.

Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs.

**Features That Use Real IP Addresses**

The following commands and features use real IP addresses in the ACLs, even if the address as seen on an interface is the mapped address:

- Access Rules (extended ACLs referenced by the `access-group` command)
- Service Policy Rules (Modular Policy Framework `match access-list` command)
- Botnet Traffic Filter traffic classification (`dynamic-filter enable classify-list` command)
- AAA Rules (`aaa ... match` commands)
- WCCP (`wccp redirect-list group-list` command)

For example, if you configure NAT for an inside server, 10.1.1.5, so that it has a publicly routable IP address on the outside, 209.165.201.5, then the access rule to allow the outside traffic to access the inside server needs to reference the server’s real IP address (10.1.1.5), and not the mapped address (209.165.201.5).

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,外界) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
hostname(config)# access-group OUTSIDE in interface outside
```

**Features That Use Mapped IP Addresses**

The following features use ACLs, but these ACLs use the mapped values as seen on an interface:

- IPsec ACLs
- `capture` command ACLs
• Per-user ACLs
• Routing protocol ACLs
• All other feature ACLs.

Time-Based ACEs

You can apply time range objects to extended and webtype ACEs so that the rules are active for specific time periods only. These types of rules let you differentiate between activity that is acceptable at certain times of the day but that is unacceptable at other times. For example, you could provide additional restrictions during working hours, and relax them after work hours or at lunch. Conversely, you could essentially shut your network down during non-work hours.

You cannot create time-based rules that have the exact same protocol, source, destination, and service criteria of a rule that does not include a time range object. The non-time-based rule always overrides the duplicate time-based rule, as they are redundant.

Note

Users could experience a delay of approximately 80 to 100 seconds after the specified end time for the ACL to become inactive. For example, if the specified end time is 3:50, because the end time is inclusive, the command is picked up anywhere between 3:51:00 and 3:51:59. After the command is picked up, the ASA finishes any currently running task and then services the command to deactivate the ACL.

Licensing for Access Control Lists

Access control lists do not require a special license.

However, to use sctp as the protocol in an entry, you must have a Carrier license.

Guidelines for ACLs

Firewall Mode

• Extended and standard ACLs are supported in routed and transparent firewall modes.
• Webtype ACLs are supported in routed mode only.
• EtherType ACLs are supported for bridge group member interfaces only, in routed and transparent modes.

Failover and Clustering

Configuration sessions are not synchronized across failover or clustered units. When you commit the changes in a session, they are made in all failover and cluster units as normal.

IPv6

• Extended and webtype ACLs allow a mix of IPv4 and IPv6 addresses.
• Standard ACLs do not allow IPv6 addresses.
• EtherType ACLs do not contain IP addresses.

Additional Guidelines

• When you specify a network mask, the method is different from the Cisco IOS software access-list command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).

• Normally, you cannot reference an object or object group that does not exist in an ACL or object group, or delete one that is currently referenced. You also cannot reference an ACL that does not exist in an access-group command (to apply access rules). However, you can change this default behavior so that you can “forward reference” objects or ACLs before you create them. Until you create the objects or ACLs, any rules or access groups that reference them are ignored. To enable forward referencing, use the forward-reference enable command.

• (Extended ACL only) The following features use ACLs, but cannot accept an ACL with identity firewall (specifying user or group names), FQDN (fully-qualified domain names), or Cisco TrustSec values:
  • VPN crypto map command
  • VPN group-policy command, except for vpn-filter
  • WCCP
  • DAP

Configure ACLs

The following sections explain how to configure the various types of ACL. Read the section on ACL basics to get the big picture, then the sections on specific types of ACL for the details.

Basic ACL Configuration and Management Options

An ACL is made up of one or more access control entries (ACEs) with the same ACL ID or name. To create a new ACL, you simply create an ACE with a new ACL name, and it becomes the first rule in the new ACL.

Working with an ACL, you can do the following things:

Examine the ACL contents and determine line numbers and hit counts

Use the show access-list name command to view the contents of the ACL. Each row is an ACE, and includes the line number, which you will need to know if you want to insert new entries into an extended ACL. The information also includes a hit count for each ACE, which is how many times the rule was matched by traffic. For example:

hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any (hitcnt=0) 0xccc48b55c
access-list outside_access_in line 2 extended permit ip host 2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
Add an ACE

The command for adding an ACE is `access-list name [line line-num] type parameters`. The line number argument works for extended ACLs only. If you include the line number, the ACE is inserted at that location in the ACL, and the ACE that was at that location is moved down, along with the remainder of the ACEs (that is, inserting an ACE at a line number does not replace the old ACE at that line). If you do not include a line number, the ACE is added to the end of the ACL. The parameters available differ based on the ACL type; see the specific topics on each ACL type for details.

Add comments to an ACL (all types except webtype)

Use the `access-list name [line line-num] remark text` command to add remarks into an ACL to help explain the purpose of an ACE. Best practice is to insert the remark before the ACE; if you view the configuration in ASDM, remarks will be associated with the ACE that follows the remarks. You can enter multiple remarks before an ACE to include an expanded comment. Each remark is limited to 100 characters. You can include leading spaces to help set off the remarks. If you do not include a line number, the remark is added to the end of the ACL. For example, you could add remarks before adding each ACE:

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

Edit or move an ACE or remark

You cannot edit or move an ACE or remark. Instead, you must create a new ACE or remark with the desired values at the right location (using the line number), then delete the old ACE or remark. Because you can insert ACEs in extended ACLs only, you need to rebuild standard, webtype, or EtherType ACLs if you need to edit or move ACEs. It is far easier to reorganize a long ACL using ASDM.

Delete an ACE or remark

Use the `no access-list parameters` command to remove an ACE or remark. Use the `show access-list` command to view the parameter string that you must enter: the string must exactly match an ACE or remark to delete it, with the exception of the `line line-num` argument, which is optional on the `no access-list` command.

Delete an entire ACL, including remarks

Use the `clear configure access-list name` command. USE CAUTION! The command does not ask you for confirmation. If you do not include a name, every access list on the ASA is removed.

Rename an ACL

Use the `access-list name rename new_name` command.

Apply the ACL to a policy

Creating an ACL in and of itself does nothing to traffic. You must apply the ACL to a policy. For example, you can use the `access-group` command to apply an extended ACL to an interface, thus denying or permitting traffic that goes through the interface.
Configure Extended ACLs

An extended ACL is composed of all ACEs with the same ACL ID or name. Extended ACLs are the most complex and feature-rich type of ACL, and you can use them for many features. The most noteworthy use of extended ACLs is as access groups applied globally or to interfaces, which determine the traffic that will be denied or permitted to flow through the box. But extended ACLs are also used to determine the traffic to which other services will be provided.

Because extended ACLs are complex, the following sections focus on creating ACEs to provide specific types of traffic matching. The first sections, on basic address-based ACEs and on TCP/UDP ACEs, build the foundation for the remaining sections.

Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching

The basic extended ACE matches traffic based on source and destination addresses, including IPv4 and IPv6 addresses and fully-qualified domain names (FQDN), such as www.example.com. In fact, every type of extended ACE must include some specification for source and destination address, so this topic explains the minimum extended ACE.

Tip If you want to match traffic based on FQDN, you must create a network object for each FQDN.

To add an ACE for IP address or FQDN matching, use the following command:

```plaintext
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument source_address_argument dest_address_argument [log [[level] [interval secs] [disable | default]] [time-range time_range_name] [inactive]
```

Example:

```plaintext
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

The options are:

- `access_list_name`—The name of the new or existing ACL.
- `line line_number`—The `line line_number` option specifies the line number at which insert the ACE; otherwise, the ACE is added to the end of the ACL.
- `deny`—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.
- `protocol_argument`—The `protocol_argument` specifies the IP protocol:
  - `name or number`—Specifies the protocol name or number. Specify `ip` to apply to all protocols.
  - `object-group protocol_grp_id`—Specifies a protocol object group created using the `object-group protocol` command.
  - `object service_obj_id`—Specifies a service object created using the `object service` command. The object can include port or ICMP type and code specifications if desired.
  - `object-group service_grp_id`—Specifies a service object group created using the `object-group service` command.
• Source Address, Destination Address—The `source_address_argument` specifies the IP address or FQDN from which the packet is being sent, and the `dest_address_argument` specifies the IP address or FQDN to which the packet is being sent:

  • **host ip_address**—Specifies an IPv4 host address.

  • **ip_address mask**—Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0.

  • **ipv6-address/prefix-length**—Specifies an IPv6 host or network address and prefix.

  • **any, any4, and any6**—`any` specifies both IPv4 and IPv6 traffic; `any4` specifies IPv4 traffic only; and `any6` specifies IPv6 traffic only.

  • **interface interface_name**—Specifies the name of an ASA interface. Use the interface name rather than IP address to match traffic based on which interface is the source or destination of the traffic.

  • **object nw_obj_id**—Specifies a network object created using the `object network` command.

  • **object-group nw_grp_id**—Specifies a network object group created using the `object-group network` command.

• Logging—`log` arguments set logging options when an ACE matches a connection for network access (an ACL applied with the `access-group` command). If you enter the `log` option without any arguments, you enable syslog message 106100 at the default level (6) and for the default interval (300 seconds). Log options are:

  • **level**—A severity level between 0 and 7. The default is 6 (informational). If you change this level for an active ACE, the new level applies to new connections; existing connections continue to be logged at the previous level.

  • **interval secs**—The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics.

  • **disable**—Disables all ACE logging.

  • **default**—Enables logging to message 106023 for denied packets. This setting is the same as not including the `log` option.

• Time Range—The `time-range time_range_name` option specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active.

• Activation—Use the `inactive` option to disable the ACE without deleting it. To reenable it, enter the entire ACE without the `inactive` keyword.

### Add an Extended ACE for Port-Based Matching

If you specify service objects in an ACE, the service objects can include protocols with port specifications, such as TCP/80. Alternatively, you can specify the ports directly in the ACE. With port-based matching, you can target certain types of traffic for port-based protocols rather than all traffic for the protocol.

The port-based extended ACE is just the basic address-matching ACE where the protocol is `tcp`, `udp`, or `sctp`. To add port specifications, use the following command:
**Add an Extended ACE for ICMP-Based Matching**

If you specify service objects in an ACE, the service objects can include the ICMP/ICMP6 protocols ICMP type and code specifications. Alternatively, you can specify the ICMP type and code directly in the ACE. For example, you can target ICMP Echo Request traffic (pings).

The ICMP extended ACE is just the basic address-matching ACE where the protocol is `icmp` or `icmp6`. Because these protocols have type and code values, you can add type and code specifications to the ACE.

To add an ACE for IP address or FQDN matching, where the protocol is ICMP or ICMP6, use the following command:
**Add an Extended ACE for User-Based Matching (Identity Firewall)**

The user-based extended ACE is just the basic address-matching ACE where you include username or user group to the source matching criteria. By creating rules based on user identity, you can avoid tying rules to static host or network addresses. For example, if you define a rule for user1, and the identity firewall feature maps that user to a host assigned 10.100.10.3 one day, but 192.168.1.5 the next day, the user-based rule still applies.

Because you must still supply source and destination addresses, broaden the source address to include the likely addresses that will be assigned to the user (normally through DHCP). For example, user “LOCAL\user1 any” will match the LOCAL\user1 user no matter what address is assigned, whereas “LOCAL\user1 10.100.1.0 255.255.255.0” matches the user only if the address is on the 10.100.1.0/24 network.

By using group names, you can define rules based on entire classes of users, such as students, teachers, managers, engineers, and so forth.

To add an ACE for user or group matching, use the following command:

```
access-list access_list_name [line line_number] extended {deny | permit} {icmp | icmp6}
source_address_argument dest_address_argument [icmp_argument] [log [level] [interval secs] | disable | default]] [time-range time_range_name] [inactive]
```

Example:

```
hostname(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

The `user_argument` option specifies the user or group for which to match traffic in addition to the source address. Available arguments include the following:

- `protocol_argument`  
  - `permit`  
  - `deny`  

- `source_address_argument`  

- `destination_address_argument`  

- `icmp_argument`  
  - `icmp_type [icmp_code]`—Specifies the ICMP type by name or number, and the optional ICMP code for that type. If you do not specify the code, then all codes are used.

- `object-group icmp_grp_id`—Specifies an object group for ICMP/ICMP6 created using the (deprecated) `object-group icmp-type` command.

You cannot specify the recommended generic service objects, where the protocol and type are defined within the object, as the ICMP argument. You specify these objects as part of the protocol argument, as explained in Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, on page 28.

For an explanation of the other keywords, see Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching, on page 28.
Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec)

The security group (Cisco TrustSec) extended ACE is just the basic address-matching ACE where you include security groups or tags to the source or destination matching criteria. By creating rules based on security groups, you can avoid tying rules to static host or network addresses. Because you must still supply source and destination addresses, broaden the addresses to include the likely addresses that will be assigned to users (normally through DHCP).

To add an ACE for security group matching, use the following command:

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument] [security_group_argument]
dest_address_argument [port_argument] [log [[level] [interval secs] | disable | default]] [inactive | time-range time_range_name]
```

Example:

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

The `security_group_argument` option specifies the security group for which to match traffic in addition to the source or destination address. Available arguments include the following:

- **object-group-security** `security_obj_grp_id`—Specifies a security object group created using the `object-group security` command.

- **security-group** `{name security_grp_id | tag security_grp_tag}`—Specifies a security group name or tag.

For an explanation of the other keywords, see *Add an Extended ACE for IP Address or Fully-Qualified Domain Name-Based Matching*, on page 28.
You can include both user and Cisco Trustsec security groups in a given ACE.

Examples for Extended ACLs

The following ACL allows all hosts (on the interface to which you apply the ACL) to go through the ASA:

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following ACL prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network for TCP-based traffic. All other addresses are permitted.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to selected hosts only, then enter a limited permit ACE. By default, all other traffic is denied unless explicitly permitted.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
```

The following ACL restricts all hosts (on the interface to which you apply the ACL) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following ACL that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

The following example temporarily disables an ACL that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based ACE, use the `time-range` command to define specific times of the day and week. Then use the `access-list extended` command to bind the time range to an ACE. The following example binds an ACE in the “Sales” ACL to a time range named “New_York_Minute.”

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host 209.165.201.1 time-range New_York_Minute
```

The following example shows a mixed IPv4/IPv6 ACL:
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0 255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4

Example of Converting Addresses to Objects for Extended ACLs

The following normal ACL that does not use object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside

If you make two network object groups, one for the inside hosts, and one for the web servers, then the configuration can be simplified and can be easily modified to add more hosts:

hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89
hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78
hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside

Configure Standard ACLs

A standard ACL is composed of all ACEs with the same ACL ID or name. Standard ACLs are used for a limited number of features, such as route maps or VPN filters. A standard ACL uses IPv4 addresses only, and defines destination addresses only.

To add a standard access list entry, use the following command:
access-list access_list_name standard {deny | permit} {any4 | host ip_address | ip_address mask}

Example:

hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0

The options are:

- **Name**—The `access_list_name` argument specifies the name of number of an ACL. Traditional numbers for standard ACLs are 1-99 or 1300-1999, but you can use any name or number. You create a new ACL if the ACL does not already exist, otherwise, you are adding the entry to the end of the ACL.

- **Permit or Deny**—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.

- **Destination Address**—The `any4` keyword matches all IPv4 addresses. The `host ip_address` argument matches a host IPv4 address. The `ip_address ip_mask` argument matches an IPv4 subnet, for example, 10.1.1.0 255.255.255.0.

---

**Configure Webtype ACLs**

Webtype ACLs are used for filtering clientless SSL VPN traffic, constraining user access to specific networks, subnets, hosts, and Web servers. If you do not define a filter, all connections are allowed. A webtype ACL is composed of all ACEs with the same ACL ID or name.

With webtype ACLs, you can match traffic based on URLs or destination addresses. A single ACE cannot mix these specifications. The following sections explain each type of ACE.

**Add a Webtype ACE for URL Matching**

To match traffic based on the URL the user is trying to access, use the following command:

`access-list access_list_name webtype {deny | permit} url {url_string | any} [log [[[level] [interval secs] | disable | default]]] [time_range time_range_name] [inactive]

Example:

hostname(config)# access-list acl_company webtype deny url http://*.example.com

The options are:

- **access_list_name**—The name of the new or existing ACL. If the ACL already exists, you are adding the ACE to the end of the ACL.

- **Permit or Deny**—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.

- **URL**—The `url` keyword specifies the URL to match. Use `url any` to match all URL-based traffic. Otherwise, enter a URL string, which can include wildcards. Following are some tips and limitations on specifying URLs:
  - Specify `any` to match all URLs.
  - ’Permit url any’ will allow all the URLs that have the format protocol://server-ip/path and will block traffic that does not match this pattern, such as port-forwarding. There should be an ACE to allow
connections to the required port (port 1494 in the case of Citrix) so that an implicit deny does not occur.

- Smart tunnel and ica plug-ins are not affected by an ACL with ‘permit url any’ because they match smart-tunnel:// and ica:// types only.

- You can use these protocols: cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp://. You can also use wildcards in the protocol; for example, htt* matches http and https, and an asterisk * matches all protocols. For example, *://*.example.com matches any type URL-based traffic to the example.com network.

- If you specify a smart-tunnel:// URL, you can include the server name only. The URL cannot contain a path. For example, smart-tunnel://www.example.com is acceptable, but smart-tunnel://www.example.com/index.html is not.

- An asterisk * matches none or any number of characters. To match any http URL, enter http://*/^.

- A question mark ? matches any one character exactly.

- Square brackets [ ] are range operators, matching any character in the range. For example, to match both http://www.cisco.com:80/ and http://www.cisco.com:81/, enter http://www.cisco.com:8[01]/.

- Logging—log arguments set logging options when an ACE matches a packet. If you enter the log option without any arguments, you enable syslog message 106102 at the default level (6) and for the default interval (300 seconds). Log options are:
  - level—A severity level between 0 and 7. The default is 6.
  - interval secs—The time interval in seconds between syslog messages, from 1 to 600. The default is 300.
  - disable—Disables all ACL logging.
  - default—Enables logging to message 106103. This setting is the same as not including the log option.

- Time Range—The time-range time_range_name option specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active.

- Activation—Use the inactive option to disable the ACE without deleting it. To reenable it, enter the entire ACE without the inactive keyword.

**Add a Webtype ACE for IP Address Matching**

You can match traffic based on the destination address the user is trying to access. The webtype ACL can include a mix of IPv4 and IPv6 addresses in addition to URL specifications.

To add a webtype ACE for IP address matching, use the following command:

```
access-list access_list_name webtype {deny | permit} tcp dest_address_argument [operator port] [log [level] [interval secs] | disable | default] [time_range time_range_name] [inactive]
```

Example:
For an explanation of keywords not explained here, see Add a Webtype ACE for URL Matching, on page 35. Keywords and arguments specific to this type of ACE include the following:

- **tcp**—The TCP protocol. Webtype ACLs match TCP traffic only.

- **Destination Address**—The `dest_address_argument` specifies the IP address to which the packet is being sent:
  - **host ip_address**—Specifies an IPv4 host address.
  - **dest_ip_address mask**—Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0.
  - **ipv6-address/prefix-length**—Specifies an IPv6 host or network address and prefix.
  - **any, any4, and any6**—`any` specifies both IPv4 and IPv6 traffic; `any4` specifies IPv4 traffic only; and `any6` specifies IPv6 traffic only.

- **operator port**—The destination port. If you do not specify ports, all ports are matched. The `port` can be the integer or name of a TCP port. The `operator` can be one of the following:
  - **lt**—less than
  - **gt**—greater than
  - **eq**—equal to
  - **neq**—not equal to
  - **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example, `range 100 200`.

### Examples for Webtype ACLs

The following example shows how to deny access to a specific company URL:

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

The following example shows how to deny access to a specific web page:

```
hostname(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

The following example shows how to deny HTTP access to any URL on a specific server through port 8080:

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

The following examples show how to use wildcards in webtype ACLs:

- The following example matches URLs such as http://www.example.com/layouts/1033:
access-list VPN-Group webtype permit url http://www.example.com/*

• The following example matches URLs such as http://www.example.com/ and http://www.example.net/:
  access-list test webtype permit url http://www.example.*

• The following example matches URLs such as http://www.example.com and ftp://zz.example.com:
  access-list test webtype permit url */ww?.e*co*/

• The following example matches URLs such as http://www.cisco.com:80 and https://www.cisco.com:81:
  access-list test webtype permit url */ww?.c*co*:8[01]/

  The range operator “[]” in the preceding example specifies that either character 0 or 1 can occur at that location.

• The following example matches URLs such as http://www.example.com and http://www.example.net:
  access-list test webtype permit url http://www.[a-z]xample?*/

  The range operator “[ ]” in the preceding example specifies that any character in the range from a to z can occur.

• The following example matches http or https URLs that include “cgi” somewhere in the file name or path.
  access-list test webtype permit url htt*:/*cgi?*

To match any http URL, you must enter http://*/ instead of http://*.

The following example shows how to enforce a webtype ACL to disable access to specific CIFS shares.

In this scenario we have a root folder named “shares” that contains two sub-folders named “Marketing_Reports” and “Sales_Reports.” We want to specifically deny access to the “shares/Marketing_Reports” folder.

  access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.

However, due to the implicit “deny all” at the end of the ACL, the above ACL makes all of the sub-folders inaccessible (“shares/Sales_Reports” and “shares/Marketing_Reports”), including the root folder (“shares”). To fix the problem, add a new ACL to allow access to the root folder and the remaining sub-folders:

  access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares/*
Configure EtherType ACLs

EtherType ACLs apply to non-IP layer-2 traffic on bridge group member interfaces. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet. With EtherType ACLs, you can control the flow of non-IP traffic across the bridge group. Note that 802.3-formatted frames are not handled by the ACL because they use a length field as opposed to a type field.

To add an EtherType ACE, use the following command:

```
access-list access_list_name ethertype \{deny | permit\} \{any | bpdu | dsap \{hex_address | bpdu | ipx | isis | raw-ipx\} | eii-ipx | ipx | isis | mpls-multicast | mpls-unicast \{hex_number\}
```

Example:

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

The options are:

- `access_list_name`—The name of the new or existing ACL. If the ACL already exists, you are adding the ACE to the end of the ACL.
- Permit or Deny—The `deny` keyword denies a packet if the conditions are matched. The `permit` keyword permits a packet if the conditions are matched.
- Traffic Matching Criteria—You can match traffic using the following options:
  - `any`—Matches all layer 2 traffic.
  - `bpdu`—bridge protocol data units (dsap 0x42), which are allowed by default. This keyword is converted to `dsap bpdu`.
  - `dsap \{hex_address | bpdu | ipx | isis | raw-ipx\}`—The IEEE 802.2 Logical Link Control (LLC) packet's Destination Service Access Point address. Include the address you want to permit or deny in hexadecimal, from 0x01 to 0xff. You can also use the following keywords to create rules for common values:
    - `bpdu` for 0x42, bridge protocol data units.
    - `ipx` for 0xe0, Internet Packet Exchange (IPX) 802.2 LLC.
    - `isis` for 0xfe, Intermediate System to Intermediate System (IS-IS).
    - `raw-ipx` for 0xff, raw IPX 802.3 format.
  - `eii-ipx`—Ethernet II IPX format, EtherType 0x8137.
  - `ipx`—Internet Packet Exchange (IPX). This keyword is a shortcut for configuring three separate rules, for `dsap ipx`, `dsap raw-ipx`, and `eii-ipx`.
  - `isis`—Intermediate System to Intermediate System (IS-IS). This keyword is converted to `dsap isis`.
  - `mpls-multicast`—MPLS multicast.
  - `mpls-unicast`—MPLS unicast.
  - `hex_number`—Any EtherType that can be identified by a 16-bit hexadecimal number 0x600 to 0xffff. See RFC 1700, “Assigned Numbers,” at http://www.ietf.org/rfc/rfc1700.txt for a list of EtherTypes.
Examples for EtherType ACLs

The following examples show how to configure EtherType ACLs, including how to apply them to an interface. For example, the following sample ACL allows common EtherTypes originating on the inside interface:

```bash
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
```

```bash
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

The following example allows some EtherTypes through the ASA, but it denies all others:

```bash
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

The following example denies traffic with EtherType 0x1256 but allows all others on both interfaces:

```bash
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

Edit ACLs in an Isolated Configuration Session

When you edit an ACL used for access rules or any other purpose, the change is immediately implemented and impacts traffic. With access rules, you can enable the transactional commit model to ensure that new rules become active only after rule compilation is complete, but the compilation happens after each ACE you edit.

If you want to further isolate the impact of editing ACLs, you can make your changes in a “configuration session,” which is an isolated mode that allows you to edit several ACEs and objects before explicitly committing your changes. Thus, you can ensure that all of your intended changes are complete before you change device behavior.

Before you begin

- You can edit ACLs that are referenced by an access-group command, but you cannot edit ACLs that are referenced by any other command. You can also edit unreferenced ACLs or create new ones.
- You can create or edit objects and object groups, but if you create one in a session, you cannot edit it in the same session. If the object is not defined as desired, you must commit your changes and then edit the object, or discard the entire session and start over.
- When you edit an ACL that is referenced by an access-group command (access rules), the transactional commit model is used when you commit the session. Thus, the ACL is completely compiled before the new ACL replaces the old version.
- If you enable forward referencing of ACL and object names (the `forward-reference enable` command), you can delete an ACL that is referenced by an access-group command (access rules), and then recreate
the ACL. When you commit changes, the new version of the ACL will be used after compilation is complete. You can also create rules that refer to objects that do not exist, or delete objects that are in use by access rules. However, you will get a commit error if you delete an object used by other rules, such as NAT.

Procedure

Step 1  
Start the session.

```
hostname# configure session session_name
hostname(config-s)#
```

If the `session_name` already exists, you open that session. Otherwise, you are creating a new session.

Use the `show configuration session` command to view the existing sessions. You can have at most 3 sessions active at a time. If you need to delete an old unused session, use the `clear configuration session session_name` command.

If you cannot open an existing session because someone else is editing it, you can clear the flag that indicates the session is being edited. Do this only if you are certain the session is not actually being edited. Use the `clear session session_name access` command to reset the flag.

Step 2  
(Uncommitted sessions only.) Make your changes. You can use the following basic commands with any of their parameters:

- `access-list`
- `object`
- `object-group`

Step 3  
Decide what to do with the session. The commands available depend on whether you have previously committed the session. Possible commands are:

- `exit`—To simply exit the session without committing or discarding changes, so that you can return later.

- `commit [noconfirm] [revert-save | config-save]`—(Uncommitted sessions only.) To commit your changes. You are asked if you want to save the session. You can save the revert session (revert-save), which lets you undo your changes using the `revert` command, or the configuration session (config-save), which includes all of the changes made in the session (allowing you to commit the same changes again if you would like to). If you save the revert or configuration session, the changes are committed, but the session remains active. You can open the session and revert or recommit the changes. You can avoid the prompt by including the `noconfirm` option and optionally, the desired save option.

- `abort`—(Uncommitted sessions only.) To abandon your changes and delete the session. If you want to keep the session, exit the session and use the `clear session session_name configuration` command, which empties the session without deleting it.

- `revert`—(Committed sessions only.) To undo your changes, returning the configuration back to what it was before you committed the session, and delete the session.
• **show configuration session** [**session_name**]—To show the changes made in the session.

---

### Monitoring ACLs

To monitor ACLs, enter one of the following commands:

- **show access-list** [**name**]—Displays the access lists, including the line number for each ACE and hit counts. Include an ACL name or you will see all access lists.

- **show running-config access-list** [**name**]—Displays the current running access-list configuration. Include an ACL name or you will see all access lists.

### History for ACLs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended, standard, webtype ACLs</td>
<td>7.0(1)</td>
<td>ACLs are used to control network access or to specify traffic for many features to act upon. An extended access control list is used for through-the-box access control and several other features. Standard ACLs are used in route maps and VPN filters. Webtype ACLs are used in clientless SSL VPN filtering. EtherType ACLs control non-IP layer 2 traffic. We introduced the following commands: <strong>access-list extended</strong>, <strong>access-list standard</strong>, <strong>access-list webtype</strong>, <strong>access-list ethertype</strong>.</td>
</tr>
<tr>
<td>Real IP addresses in extended ACLs</td>
<td>8.3(1)</td>
<td>When using NAT or PAT, mapped addresses and ports are no longer used in an ACL for several features. You must use the real, untranslated addresses and ports for these features. Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs.</td>
</tr>
<tr>
<td>Support for Identity Firewall in extended ACLs</td>
<td>8.4(2)</td>
<td>You can now use identity firewall users and groups for the source and destination. You can use an identity firewall ACL with access rules, AAA rules, and for VPN authentication. We modified the following commands: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>EtherType ACL support for IS-IS traffic</td>
<td>8.4(5), 9.1(2)</td>
<td>In transparent firewall mode, the ASA can now control IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype {permit</td>
</tr>
<tr>
<td>Support for Cisco TrustSec in extended ACLs</td>
<td>9.0(1)</td>
<td>You can now use Cisco TrustSec security groups for the source and destination. You can use an identity firewall ACL with access rules. We modified the following commands: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unified extended and webtype ACLs for IPv4 and IPv6</td>
<td>9.0(1)</td>
<td>Extended and webtype ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The any keyword was changed to represent IPv4 and IPv6 traffic. The any4 and any6 keywords were added to represent IPv4-only and IPv6-only traffic, respectively. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. We modified the following commands: <strong>access-list extended</strong>, <strong>access-list webtype</strong>. We removed the following commands: <strong>ipv6 access-list</strong>, <strong>ipv6 access-list webtype</strong>, <strong>ipv6-vpn-filter</strong>.</td>
</tr>
<tr>
<td>Extended ACL and object enhancement to filter ICMP traffic by ICMP code</td>
<td>9.0(1)</td>
<td>ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: <strong>access-list extended</strong>, <strong>service-object</strong>, <strong>service</strong>.</td>
</tr>
<tr>
<td>Configuration session for editing ACLs and objects. Forward referencing of objects and ACLs in access rules.</td>
<td>9.3(2)</td>
<td>You can now edit ACLs and objects in an isolated configuration session. You can also forward reference objects and ACLs, that is, configure rules and access groups for objects or ACLs that do not yet exist. We introduced the <strong>clear configuration session</strong>, <strong>clear session</strong>, <strong>configure session</strong>, <strong>forward-reference</strong>, and <strong>show configuration session</strong> commands.</td>
</tr>
<tr>
<td>ACL support for Stream Control Transmission Protocol (SCTP)</td>
<td>9.5(2)</td>
<td>You can now create ACL rules using the <strong>setp</strong> protocol, including port specifications. We modified the following command: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>Ethertype rule support for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address.</td>
<td>9.6(2)</td>
<td>You can now write Ethertype access control rules for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Because of this addition, the <strong>bdpu</strong> keyword no longer matches the intended traffic. Rewrite <strong>bdpu</strong> rules for <strong>dsap 0x42</strong>. We modified the following commands: <strong>access-list ethertype</strong>.</td>
</tr>
<tr>
<td>Support in routed mode for Ethertype rules on bridge group member interfaces and extended access rules on Bridge Group Virtual Interfaces (BVI).</td>
<td>9.7(1)</td>
<td>You can now create Ethertype ACLs and apply them to bridge group member interfaces in routed mode. You can also apply extended access rules to the Bridge Virtual Interface (BVI) in addition to the member interfaces. We modified the following commands: <strong>access-group</strong>, <strong>access-list ethertype</strong>.</td>
</tr>
</tbody>
</table>
 EtherType access control list changes.  9.9(1)  EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access control entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes.

We modified the following commands: access-list ethertype added the new keywords eii-ipx and dsap {bpdu | ipx | isis | raw-ipx}; capture ethernet-type no longer supports the ipx keyword.
CHAPTER 4

Access Rules

This chapter describes how to control network access through or to the ASA using access rules. 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 ASA 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 the general operations configuration guide.

- Controlling Network Access, on page 45
- Licensing for Access Rules, on page 50
- Guidelines for Access Control, on page 51
- Configure Access Control, on page 52
- Monitoring Access Rules, on page 54
- Configuration Examples for Permitting or Denying Network Access, on page 56
- History for Access Rules, on page 57

Controlling Network Access

Access rules determine which traffic is allowed through the ASA. There are several different layers of rules that work together to implement your access control policy:

- Extended access rules (Layer 3+ traffic) assigned to interfaces—You can apply separate rule sets (ACLs) in the inbound and outbound directions. An extended access rule permits or denies traffic based on the source and destination traffic criteria.

- Extended access rules (Layer 3+ traffic) assigned to Bridge Virtual Interfaces (BVI; routed mode)—If you name a BVI, you can apply separate rule sets in the inbound and outbound direction, and you can also apply rule sets to the bridge group member interfaces. When both the BVI and member interface have access rules, the order of processing depends on direction. Inbound, the member access rules are evaluated first, then the BVI access rules. Outbound, the BVI rules are considered first, then the member interface rules.

- Extended access rules assigned globally—You can create a single global rule set, which serves as your default access control. The global rules are applied after interface rules.
• Management access rules (Layer 3+ traffic)—You can apply a single rule set to cover traffic directed at an interface, which would typically be management traffic. In the CLI, these are “control plane” access groups. For ICMP traffic directed at the device, you can alternatively configure ICMP rules.

• EtherType rules (Layer 2 traffic) assigned to interfaces (bridge group member interfaces only)—You can apply separate rule sets in the inbound and outbound directions. EtherType rules control network access for non-IP traffic. An EtherType rule permits or denies traffic based on the EtherType. You can also apply extended access rules to bridge group member interfaces to control Layer 3+ traffic.

General Information About Rules

The following topics provide general information about access rules and EtherType rules.

Interface Access Rules and Global Access Rules

You can apply an access rule to a specific interface, or you can apply an access rule globally to all interfaces. You can configure global access rules in conjunction with interface access rules, in which case, the specific inbound interface access rules are always processed before the general global access rules. Global access rules apply only to inbound traffic.

Inbound and Outbound Rules

You can configure access rules based on the direction of traffic:

• Inbound—Inbound access rules apply to traffic as it enters an interface. Global and management access rules are always inbound.

• Outbound—Outbound rules apply to traffic as it exits an interface.

Note

“Inbound” and “outbound” refer to the application of an ACL on an interface, either to traffic entering the ASA on an interface or traffic exiting the ASA 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 ACL 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 ACLs to restrict access, you can create a single outbound ACL that allows only the specified hosts. (See the following figure.) The outbound ACL prevents any other hosts from reaching the outside network.
See the following commands for this example:

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

**Rule Order**

The order of rules is important. When the ASA decides whether to forward or drop a packet, the ASA tests the packet against each rule in the order in which the rules are listed in the applied ACL. 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.

**Implicit Permits**

Unicast IPv4 and IPv6 traffic from a higher security interface to a lower security interface is allowed through by default. This includes traffic between standard routed interfaces and Bridge Virtual Interfaces (BVI) in routed mode.

For bridge group member interfaces, this implicit permit from a higher to a lower security interface applies to interfaces within the same bridge group only. There are no implicit permits between a bridge group member interface and a routed interface or a member of a different bridge group.
Bridge group member interfaces (routed or transparent mode) also allow the following by default:

- ARPs in both directions. (You can control ARP traffic using ARP inspection, but you cannot control it by access rule.)
- BPDUs in both directions. (You can control these using Ethertype rules.)

For other traffic, you need to use either an extended access rule (IPv4 and IPv6) or an EtherType rule (non-IP).

**Implicit Deny**

ACLs 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 ASA except for particular addresses, then you need to deny the particular addresses and then permit all others.

For management (control plane) ACLs, which control to-the-box traffic, there is no implicit deny at the end of a set of management rules for an interface. Instead, any connection that does not match a management access rule is then evaluated by regular access control rules.

For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (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; only physical protocol traffic, such as auto-negotiation, is still allowed.

If you configure a global access rule, then the implicit deny comes after the global rule is processed. See the following order of operations:

1. Interface access rule.
2. For bridge group member interfaces, the Bridge Virtual Interface (BVI) access rule.
3. Global access rule.
4. Implicit deny.

**NAT and Access Rules**

Access rules always use the real IP addresses when determining an access rule match, even if you configure NAT. For example, if you configure NAT for an inside server, 10.1.1.5, so that it has a publicly routable IP address on the outside, 209.165.201.5, then the access rule to allow the outside traffic to access the inside server needs to reference the server’s real IP address (10.1.1.5), and not the mapped address (209.165.201.5).

**Extended Access Rules**

This section describes information about extended access rules.

**Extended Access Rules for Returning Traffic**

For TCP, UDP, and SCTP connections for both routed and transparent mode, you do not need an access rule to allow returning traffic because the ASA allows all returning traffic for established, bidirectional connections.

For connectionless protocols such as ICMP, however, the ASA establishes unidirectional sessions, so you either need access rules to allow ICMP in both directions (by applying ACLs 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. For example, to control ping, specify `echo-reply (0)` (ASA to host) or `echo (8)` (host to ASA).

Allowing Broadcast and Multicast Traffic

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. You must configure the dynamic routing protocols or DHCP relay to allow this traffic.

For interfaces that are members of the same bridge group in transparent or routed firewall mode, you can allow any IP traffic through using access rules.

---

**Note**

Because these special types of traffic are connectionless, you need to apply an access rule to both the inbound and outbound interfaces, so returning traffic is allowed through.

The following table lists common traffic types that you can allow using access rules between interfaces that are members of the same bridge group.

**Table 2: Special Traffic for Access Rules between Members of the Same Bridge Group**

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Protocol or Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>UDP ports 67 and 68</td>
<td>If you enable the DHCP server, then the ASA does not pass DHCP packets.</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Protocol 88</td>
<td>—</td>
</tr>
<tr>
<td>OSPF</td>
<td>Protocol 89</td>
<td>—</td>
</tr>
<tr>
<td>Multicast streams</td>
<td>The UDP ports vary depending on the application.</td>
<td>Multicast streams are always destined to a Class D address (224.0.0.0 to 239.x.x.x).</td>
</tr>
<tr>
<td>RIP (v1 or v2)</td>
<td>UDP port 520</td>
<td>—</td>
</tr>
</tbody>
</table>

Management Access Rules

You can configure access rules that control management traffic destined to the ASA. Access control rules for to-the-box management traffic (defined by such commands as `http`, `ssh`, or `telnet`) have higher precedence than a management access rule applied with the `control-plane` option. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box ACL.

Unlike regular access rules, there is no implicit deny at the end of a set of management rules for an interface. Instead, any connection that does not match a management access rule is then evaluated by regular access control rules.

Alternatively, you can use ICMP rules to control ICMP traffic to the device. Use regular extended access rules to control ICMP traffic through the device.

EtherType Rules

This section describes EtherType rules.
**Supported EtherTypes and Other Traffic**

An EtherType rule controls the following:

- EtherType identified by a 16-bit hexadecimal number, including common types IPX and MPLS unicast or multicast.
- Ethernet V2 frames.
- BPDUs, which are permitted by default. BPDUs are SNAP-encapsulated, and the ASA is designed to specifically handle BPDUs.
- Trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the ASA modifies the payload with the outgoing VLAN if you allow BPDUs.
- The IEEE 802.2 Logical Link Control packet. You can control access based on the Destination Service Access Point address.

The following types of traffic are not supported:

- 802.3-formatted frames—These frames are not handled by the rule because they use a length field as opposed to a type field.

**EtherType Rules for Returning Traffic**

Because EtherTypes are connectionless, you need to apply the rule to both interfaces if you want traffic to pass in both directions.

**Allowing MPLS**

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the ASA by configuring both MPLS routers connected to the ASA to use the IP address on the ASA 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 ASA.

```plaintext
mpls ldp router-id interface force
```

Or

```plaintext
tag-switching tdp router-id interface force
```

**Licensing for Access Rules**

Access control rules do not require a special license.

However, to use `sctp` as the protocol in a rule, you must have a Carrier license.
Guidelines for Access Control

IPv6 Guidelines

Supports IPv6. The source and destination addresses can include any mix of IPv4 and IPv6 addresses.

Per-User ACL Guidelines

• The per-user ACL uses the value in the `timeout uauth` command, but it can be overridden by the AAA per-user session timeout value.

• If traffic is denied because of a per-user ACL, syslog message 109025 is logged. If traffic is permitted, no syslog message is generated. The `log` option in the per-user ACL has no effect.

Additional Guidelines and Limitations

• You can reduce the memory required to search access rules by enabling object group search, but this is at the expense of lookup performance and increased CPU utilization. When enabled, object group search does not expand network or service objects, but instead searches access rules for matches based on those group definitions. You can set this option using the `object-group-search access-control` command.

For each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. This check is to prevent performance degradation. Configure your rules to prevent an excessive number of matches.

Note

Object group search works with network and service objects only. It does not work with security group or user objects. Do not enable this feature if the ACLs include security groups. The result can be inactive ACLs or other unexpected behavior.

• You can improve system performance and reliability by using the transactional commit model for access groups. See the basic settings chapter in the general operations configuration guide for more information. Use the `asp rule-engine transactional-commit access-group` command.

• In ASDM, rule descriptions are based on the access list remarks that come before the rule in the ACL; for new rules you create in ASDM, any descriptions are also configured as remarks before the related rule. However, the packet tracer in ASDM matches the remark that is configured after the matching rule in the CLI.

• Normally, you cannot reference an object or object group that does not exist in an ACL or object group, or delete one that is currently referenced. You also cannot reference an ACL that does not exist in an `access-group` command (to apply access rules). However, you can change this default behavior so that you can “forward reference” objects or ACLs before you create them. Until you create the objects or ACLs, any rules or access groups that reference them are ignored. To enable forward referencing, use the `forward-reference enable` command.
Configure Access Control

The following topics explain how to configure access control.

Configure an Access Group

Before you can create an access group, create the ACL.

To bind an ACL to an interface or to apply it globally, use the following command:

```
access-group access_list { [in | out] interface interface_name [per-user-override | control-plane] | global }
```

For an interface-specific access group:

- Specify the extended or EtherType ACL name. You can configure one `access-group` command per ACL type per interface per direction, and one control plane ACL. The control plane ACL must be an extended ACL. Ethertype ACLs are allowed on bridge group member interfaces only. For bridge groups in routed mode, you can specify extended ACLs for each direction on both the Bridge Virtual Interface (BVI) and each bridge group member interface.

- The `in` keyword applies the ACL to inbound traffic. The `out` keyword applies the ACL to the outbound traffic.

- Specify the `interface` name.

- The `per-user-override` keyword (for inbound extended ACLs only) allows dynamic user ACLs that are downloaded for user authorization to override the ACL assigned to the interface. For example, if the interface ACL denies all traffic from 10.0.0.0, but the dynamic ACL permits all traffic from 10.0.0.0, then the dynamic ACL overrides the interface ACL for that user.

By default, VPN remote access traffic is not matched against interface ACLs. However, if you use the `no sysopt connection permit-vpn` command to turn off this bypass, the behavior depends on whether there is a `vpn-filter` applied in the group policy and whether you set the `per-user-override` option:

- **No `per-user-override`, no `vpn-filter`**—Traffic is matched against the interface ACL.

- **No `per-user-override`, `vpn-filter`**—Traffic is matched first against the interface ACL, then against the VPN filter.

- **`per-user-override`, `vpn-filter`**—Traffic is matched against the VPN filter only.

- The `control-plane` keyword specifies if the extended ACL is for to-the-box traffic.

Unlike regular access rules, there is no implicit deny at the end of a set of management (control plane) rules for an interface. Instead, any connection that does not match a management access rule is then evaluated by regular access control rules.

For a global access group, specify the `global` keyword to apply the extended ACL to the inbound direction of all interfaces.

Example

The following example shows how to use the `access-group` command:
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside

The **access-list** command lets any host access the host address using port 80. The **access-group** command specifies that the **access-list** command applies to traffic entering the outside interface.

## Configure ICMP Access Rules

By default, you can send ICMP packets to any interface using either IPv4 or IPv6, with these exceptions:

- The ASA does not respond to ICMP echo requests directed to a broadcast address.
- The ASA only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

To protect the device from attacks, you can use ICMP rules to limit ICMP access to interfaces to particular hosts, networks, or ICMP types. ICMP rules function like access rules, where the rules are ordered, and the first rule that matches a packet defines the action.

If you configure any ICMP rule for an interface, an implicit deny ICMP rule is added to the end of the ICMP rule list, changing the default behavior. Thus, if you want to simply deny a few message types, you must include a permit any rule at the end of the ICMP rule list to allow the remaining message types.

We recommend that you always grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. Additionally ICMP packets in IPv6 are used in the IPv6 neighbor discovery process.

### Procedure

**Step 1** Create rules for ICMP traffic.

```
icmp {permit | deny} {host ip_address | ip_address mask | any} [icmp_type] interface_name
```

If you do not specify an **icmp_type**, the rule applies to all types. You can enter the number or the name. To control ping, specify echo-reply (0) (ASA-to-host) or echo (8) (host-to-ASA).

For the address, you can apply the rule to **any** address, to a single **host**, or to a network (**ip_address mask**).

**Step 2** Create rules for ICMPv6 (IPv6) traffic.

```
ipv6 icmp {permit | deny} {host ipv6_address | ipv6-network/prefix-length | any} [icmp_type] interface_name
```

If you do not specify an **icmp_type**, the rule applies to all types.

For the address, you can apply the rule to **any** address, to a single **host**, or to a network (**ipv6-network/prefix-length**).

**Step 3** (Optional.) Set rate limits on ICMP Unreachable messages so that the ASA will appear on trace route output.

```
icmp unreachable rate-limit rate burst-size size
```

The rate limit can be 1-100, with 1 being the default. The burst size is meaningless, but must be 1-10.

**Example:**

```
Increasing the rate limit, along with enabling the `set connection decrement-ttl` command in a service policy, is required to allow a traceroute through the ASA that shows the ASA as one of the hops. For example, the following policy increases the rate limit and decrements the time-to-live (TTL) value for all traffic through the ASA.

```
icmp unreachable rate-limit 50 burst-size 1
class-map global-class
    match any
policy-map global_policy
    class global-class
        set connection decrement-ttl
```

**Examples**

The following example shows how to allow all hosts except the one at 10.1.1.15 to use ICMP to the inside interface:

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

The following example shows how to allow the host at 10.1.1.15 to use only ping to the inside interface:

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

The following example shows how to deny all ping requests and permit all packet-too-big messages (to support path MTU discovery) at the outside interface:

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

The following example shows how to permit host 2000::0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
hostname(config)# ipv6 icmp permit host 2000::0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

**Monitoring Access Rules**

To monitor network access, enter the following commands:

- `clear access-list id counters`
  - Clear the hit counts for the access list.
- `show access-list [name]`
Displays the access lists, including the line number for each ACE and hit counts. Include an ACL name or you will see all access lists.

- `show running-config access-group`

  Displays the current ACL bound to the interfaces.

### Evaluating Syslog Messages for Access Rules

Use a syslog event viewer, such as the one in ASDM, to view messages related to access rules.

If you use default logging, you see syslog message 106023 for explicitly denied flows only. Traffic that matches the “implicit deny” entry that ends the rule list is not logged.

If the ASA is attacked, the number of syslog messages for denied packets can be very large. We recommend that you instead enable logging using syslog message 106100, which provides statistics for each rule (including permit rules) and enables you to limit the number of syslog messages produced. Alternatively, you can disable all logging for a given rule.

When you enable logging for message 106100, if a packet matches an ACE, the ASA creates a flow entry to track the number of packets received within a specific interval. The ASA generates a syslog message at the first hit and at the end of each interval, identifying the total number of hits during the interval and the time stamp for the last hit. At the end of each interval, the ASA resets the hit count to 0. If no packets match the ACE during an interval, the ASA deletes the flow entry. When you configure logging for a rule, you can control the interval and even the severity level of the log message, per rule.

A flow is defined by the source and destination IP addresses, protocols, and ports. Because the source port might differ for a new connection between the same two hosts, you might not see the same flow increment because a new flow was created for the connection.

Permitted packets that belong to established connections do not need to be checked against ACLs; only the initial packet is logged and included in the hit count. For connectionless protocols, such as ICMP, all packets are logged, even if they are permitted, and all denied packets are logged.

See the [syslog messages guide](#) for detailed information about these messages.

---

**Tip**

When you enable logging for message 106100, if a packet matches an ACE, the ASA creates a flow entry to track the number of packets received within a specific interval. The ASA has a maximum of 32 K logging flows for ACEs. A large number of flows can exist concurrently at any point of time. To prevent unlimited consumption of memory and CPU resources, the ASA places a limit on the number of concurrent deny flows; the limit is placed on deny flows only (not on permit flows) because they can indicate an attack. When the limit is reached, the ASA does not create a new deny flow for logging until the existing flows expire, and issues message 106101. You can control the frequency of this message using the `access-list alert-interval secs` command, and the maximum number of deny flows cached using the `access-list deny-flow-max number` command.
Configuration Examples for Permitting or Denying Network Access

Following are some typical configuration examples for permitting or denying network access.

Extended ACL Examples

The following example adds a network object for inside server 1, performs static NAT for the server, and enables access from the outside for inside server 1.

```bash
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12
hostname(config)# access-list outside_access extended permit tcp any object inside-server1 eq www
hostname(config)# access-group outside_access in interface outside
```

The following example allows all hosts to communicate between the inside and hr networks but only specific hosts to access the outside network:

```bash
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

The following example uses object groups to permit specific traffic on the inside interface:

```bash
! hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destination
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo
hostname(config)# access-list outsideacl extended permit object-group myaclog interface inside any
```

EtherType Examples

For example, the following sample ACL allows common EtherTypes originating on the inside interface:

```bash
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```
The following example allows some EtherTypes through the ASA, but it denies all others:

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

The following example denies traffic with EtherType 0x1256 but allows all others on both interfaces:

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

## History for Access Rules

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface access rules</td>
<td>7.0(1)</td>
<td>Controlling network access through the ASA using ACLs. We introduced the following command: <strong>access-group</strong>.</td>
</tr>
<tr>
<td>Global access rules</td>
<td>8.3(1)</td>
<td>Global access rules were introduced. We modified the following command: <strong>access-group</strong>.</td>
</tr>
<tr>
<td>Support for Identity Firewall</td>
<td>8.4(2)</td>
<td>You can now use identity firewall users and groups for the source and destination. You can use an identity firewall ACL with access rules, AAA rules, and for VPN authentication. We modified the following commands: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>EtherType ACL support for IS-IS traffic</td>
<td>8.4(5), 9.1(2)</td>
<td>In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: **access-list ethertype {permit</td>
</tr>
<tr>
<td>Support for TrustSec</td>
<td>9.0(1)</td>
<td>You can now use TrustSec security groups for the source and destination. You can use an identity firewall ACL with access rules. We modified the following commands: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Unified ACL for IPv4 and IPv6</td>
<td>9.0(1)</td>
<td>ACLs now support IPv4 and IPv6 addresses. You can even specify a mix of IPv4 and IPv6 addresses for the source and destination. The <em>any</em> keyword was changed to represent IPv4 and IPv6 traffic. The <em>any4</em> and <em>any6</em> keywords were added to represent IPv4-only and IPv6-only traffic, respectively. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. We modified the following commands: <strong>access-list extended, access-list webtype</strong>. We removed the following commands: <strong>ipv6 access-list, ipv6 access-list webtype, ipv6-vpn-filter</strong>.</td>
</tr>
<tr>
<td>Extended ACL and object enhancement to filter ICMP traffic by ICMP code</td>
<td>9.0(1)</td>
<td>ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following commands: <strong>access-list extended, service-object, service</strong>.</td>
</tr>
<tr>
<td>Transactional Commit Model on Access Group Rule Engine</td>
<td>9.1(5)</td>
<td>When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We introduced the following commands: <strong>asp rule-engine transactional-commit, show running-config asp rule-engine transactional-commit, clear configure asp rule-engine transactional-commit</strong>.</td>
</tr>
<tr>
<td>Configuration session for editing ACLs and objects. Forward referencing of objects and ACLs in access rules.</td>
<td>9.3(2)</td>
<td>You can now edit ACLs and objects in an isolated configuration session. You can also forward reference objects and ACLs, that is, configure rules and access groups for objects or ACLs that do not yet exist. We introduced the <strong>clear config-session, clear session, configure session, forward-reference, and show config-session</strong> commands.</td>
</tr>
<tr>
<td>Access rule support for Stream Control Transmission Protocol (SCTP)</td>
<td>9.5(2)</td>
<td>You can now create access rules using the <em>sctp</em> protocol, including port specifications. We modified the following command: <strong>access-list extended</strong>.</td>
</tr>
<tr>
<td>Ethertype rule support for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address.</td>
<td>9.6(2)</td>
<td>You can now write Ethertype access control rules for the IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Because of this addition, the <em>bpdu</em> keyword no longer matches the intended traffic. Rewrite <em>bpdu</em> rules for <em>dsap 0x42</em>. We modified the following commands: <strong>access-list ethertype</strong>.</td>
</tr>
<tr>
<td>Support in routed mode for Ethertype rules on bridge group member interfaces and extended access rules on Bridge Group Virtual Interfaces (BVI).</td>
<td>9.7(1)</td>
<td>You can now create Ethertype ACLs and apply them to bridge group member interfaces in routed mode. You can also apply extended access rules to the Bridge Virtual Interface (BVI) in addition to the member interfaces. We modified the following commands: <strong>access-group, access-list ethertype</strong>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| EtherType access control list changes. | 9.9(1) | EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xEE), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access control entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes.

We modified the following commands: `access-list ethertype` added the new keywords `eii-ipx` and `dsap {bpdu | ipx | isis | raw-ipx}`; `capture ethernet-type` no longer supports the `ipx` keyword. |
Identity Firewall

This chapter describes how to configure the ASA for the Identity Firewall.

- About the Identity Firewall, on page 61
- Guidelines for the Identity Firewall, on page 67
- Prerequisites for the Identity Firewall, on page 69
- Configure the Identity Firewall, on page 70
- Collect User Statistics, on page 79
- Examples for the Identity Firewall, on page 80
- Monitoring the Identity Firewall, on page 82
- History for the Identity Firewall, on page 83

**About the Identity Firewall**

In an enterprise, users often need access to one or more server resources. Typically, a firewall is not aware of the users’ identities and, therefore, cannot apply security policies based on identity. To configure per-user access policies, you must configure a user authentication proxy, which requires user interaction (a username/password query).

The Identity Firewall in the ASA provides more granular access control based on users’ identities. You can configure access rules and security policies based on user names and user group names rather than through source IP addresses. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of network IP addresses.

The Identity Firewall integrates with Microsoft Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses and allows transparent authentication for Active Directory users.

Identity-based firewall services enhance the existing access control and security policy mechanisms by allowing users or groups to be specified in place of source IP addresses. Identity-based security policies can be interleaved without restriction between traditional IP address-based rules.

The key benefits of the Identity Firewall include:

- Decoupling network topology from security policies
- Simplifying the creation of security policies
• Providing the ability to easily identify user activities on network resources
• Simplifying user activity monitoring

Architecture for Identity Firewall Deployments

The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping.

The identity firewall consists of three components:

• ASA

• Microsoft Active Directory

Although Active Directory is part of the Identity Firewall on the ASA, Active Directory administrators manage it. The reliability and accuracy of the data depends on data in Active Directory.


• Active Directory (AD) Agent


Note
Windows 2003 R2 is not supported for the AD Agent server.

The following figure shows the components of the Identity Firewall. The succeeding table describes the roles of these components and how they communicate with one another.

Figure 3: Identity Firewall Components
|   | **On the ASA:**  
|   | Administrators configure local user groups and Identity Firewall policies.  
| 1 |  
| 2 | **ASA <-> AD Server:** The ASA sends an LDAP query for the Active Directory groups configured on the AD Server.  
|   | The ASA consolidates local and Active Directory groups and applies access rules and Modular Policy Framework security policies based on user identity.  
| 3 | **ASA <-> AD Agent:** Depending on the Identity Firewall configuration, the ASA downloads the IP-user database or sends a RADIUS request to the AD Agent that asks for the user’s IP address.  
|   | The ASA forwards the new mapped entries that have been learned from web authentication and VPN sessions to the AD Agent.  
| 4 | **Client <-> ASA:** The client logs into the network through Microsoft Active Directory. The AD Server authenticates users and generates user login security logs.  
|   | Alternatively, the client can log into the network through a cut-through proxy or VPN.  
| 5 | **ASA <-> Client:** Based on the policies configured on the ASA, it grants or denies access to the client.  
|   | If configured, the ASA probes the NetBIOS of the client to pass inactive and no-response users.  
| 6 | **AD Agent <-> AD Server:** The AD Agent maintains a cache of user ID and IP address mapped entries, and notifies the ASA of changes.  
|   | The AD Agent sends logs to a syslog server.  

### Features of the Identity Firewall

The Identity Firewall includes the following key features.
Flexibility

- The ASA can retrieve user identity and IP address mapping from the AD Agent by querying the AD Agent for each new IP address or by maintaining a local copy of the entire user identity and IP address database.
- Supports host group, subnet, or IP address for the destination of a user identity policy.
- Supports a fully qualified domain name (FQDN) for the source and destination of a user identity policy.
- Supports the combination of 5-tuple policies with ID-based policies. The identity-based feature works in tandem with the existing 5-tuple solution.
- Supports use with IPS and Application Inspection policies.
- Retrieves user identity information from remote access VPN, AnyConnect VPN, L2TP VPN and cut-through proxy. All retrieved users are populated to all ASAs that are connected to the AD Agent.

Scalability

- Each AD Agent supports 100 ASAs. Multiple ASAs are able to communicate with a single AD Agent to provide scalability in larger network deployments.
- Supports 30 Active Directory servers provided the IP address is unique among all domains.
- Each user identity in a domain can have up to 8 IP addresses.
- Supports up to 64,000 user identity-IP address mapped entries in active policies for the ASA 5500 Series models. This limit controls the maximum number of users who have policies applied. The total number of users are the aggregate of all users configured in all different contexts.
- Supports up to 512 user groups in active ASA policies.
- A single access rule can contain one or more user groups or users.
- Supports multiple domains.

Availability

- The ASA retrieves group information from the Active Directory and falls back to web authentication for IP addresses when the AD Agent cannot map a source IP address to a user identity.
- The AD Agent continues to function when any of the Active Directory servers or the ASA are not responding.
- Supports configuring a primary AD Agent and a secondary AD Agent on the ASA. If the primary AD Agent stops responding, the ASA can switch to the secondary AD Agent.
- If the AD Agent is unavailable, the ASA can fall back to existing identity sources such as cut-through proxy and VPN authentication.
- The AD Agent runs a watchdog process that automatically restarts its services when they are down.
- Allows a distributed IP address/user mapping database for use among ASAs.
Deployment Scenarios

You can deploy the components of the Identity Firewall in the following ways, depending on your environmental requirements.

The following figure shows how you can deploy the components of the Identity Firewall to allow for redundancy. Scenario 1 shows a simple installation without component redundancy. Scenario 2 also shows a simple installation without redundancy. However, in this deployment scenario, the Active Directory server and AD Agent are co-located on the same Windows server.

*Figure 4: Deployment Scenario without Redundancy*

---

The following figure shows how you can deploy the Identity Firewall components to support redundancy. Scenario 1 shows a deployment with multiple Active Directory servers and a single AD Agent installed on a separate Windows server. Scenario 2 shows a deployment with multiple Active Directory servers and multiple AD Agents installed on separate Windows servers.

*Figure 5: Deployment Scenario with Redundant Components*

---

The following figure shows how all Identity Firewall components—Active Directory server, the AD Agent, and the clients—are installed and communicate on the LAN.
The following figure shows a WAN-based deployment to support a remote site. The Active Directory server and the AD Agent are installed on the main site LAN. The clients are located at a remote site and connect to the Identity Firewall components over a WAN.

The following figure also shows a WAN-based deployment to support a remote site. The Active Directory server is installed on the main site LAN. However, the AD Agent is installed and accessed by the clients at the remote site. The remote clients connect to the Active Directory servers at the main site over a WAN.
The following figure shows an expanded remote site installation. An AD Agent and Active Directory servers are installed at the remote site. The clients access these components locally when logging into network resources located at the main site. The remote Active Directory server must synchronize its data with the central Active Directory servers located at the main site.

**Figure 8: WAN-based Deployment with Remote AD Agent**

**Figure 9: WAN-based Deployment with Remote AD Agent and AD Servers**

**Guidelines for the Identity Firewall**

This section describes the guidelines and limitations that you should check before configuring the Identity Firewall.

**Failover**

- The Identity Firewall supports user identity-IP address mapping and AD Agent status replication from active to standby when Stateful Failover is enabled. However, only user identity-IP address mapping, AD Agent status, and domain status are replicated. User and user group records are not replicated to the standby ASA.

- When failover is configured, the standby ASA must also be configured to connect to the AD Agent directly to retrieve user groups. The standby ASA does not send NetBIOS packets to clients even when the NetBIOS probing options are configured for the Identity Firewall.
• When a client is determined to be inactive by the active ASA, the information is propagated to the standby ASA. User statistics are not propagated to the standby ASA.

• When you have failover configured, you must configure the AD Agent to communicate with both the active and standby ASAs. See the Installation and Setup Guide for the Active Directory Agent for the steps to configure the ASA on the AD Agent server.

**IPv6**

• The AD Agent supports endpoints with IPv6 addresses. It can receive IPv6 addresses in log events, maintain them in its cache, and send them through RADIUS messages. The AAA server must use an IPv4 address.

• NetBIOS over IPv6 is not supported.

**Additional Guidelines**

• A full URL as a destination address is not supported.

• For NetBIOS probing to function, the network between the ASA, AD Agent, and clients must support UDP-encapsulated NetBIOS traffic.

• MAC address checking by the Identity Firewall does not work when intervening routers are present. Users logged into clients that are behind the same router have the same MAC addresses. With this implementation, all the packets from the same router are able to pass the check, because the ASA is unable to ascertain the actual MAC addresses behind the router.

• Although you can use user specifications in VPN filter ACLs, the user-based rules are interpreted uni-directionally rather than bi-directionally, which is how VPN filter usually works. That is, you can filter based on user-initiated traffic, but the filter does not apply for going from the destination back to the user. For example, you could include a rule that allows a specific user to ping a server, but that rule will not allow the server to ping the user.

• The following ASA features do not support using the identity-based object and FQDN in an extended ACL:
  - Crypto maps
  - WCCP
  - NAT
  - Group policy (except for VPN filters)
  - DAP

• You can use the `user-identity update active-user-database` command to actively initiate a user-IP address download from the AD agent.

By design, if a previous download session has finished, the ASA does not allow you to issue this command again.

As a result, if the user-IP database is very large, the previous download session is not finished yet, and you issue another `user-identity update active-user-database` command, the following error message appears:
“ERROR: one update active-user-database is already in progress.”

You need to wait until the previous session is completely finished, then you can issue another `user-identity update active-user-database` command.

Another example of this behavior occurs because of packet loss from the AD Agent to the ASA.

When you issue a `user-identity update active-user-database` command, the ASA requests the total number of user-IP mapped entries to be downloaded. Then the AD Agent initiates a UDP connection to the ASA and sends the change of authorization request packet.

If for some reason the packet is lost, there is no way for the ASA to discern this. As a result, the ASA holds the session for 4-5 minutes, during which time this error message continues to appear if you have issued the `user-identity update active-user-database` command.

- When you use the Cisco Context Directory Agent (CDA) in conjunction with the ASA or Cisco Ironport Web Security Appliance (WSA), make sure that you open the following ports:
  - Authentication port for UDP—1645
  - Accounting port for UDP—1646
  - Listening port for UDP—3799

  The listening port is used to send change of authorization requests from the CDA to the ASA or to the WSA.

- If the `user-identity action domain-controller-down domain_name disable user-identity-rule` command is configured and the specified domain is down, or if the `user-identity action ad-agent-down disable user-identity-rule` command is configured and the AD Agent is down, all the logged-in users have the disabled status.

- For domain names, the following characters are not valid: \/:*?"<>|.
- For usernames, the following characters are not valid: \(/\:\+*?"<>|\[@.
- For user group names, the following characters are not valid: \(/\:\+*?"<>|.
- How you configure the Identity Firewall to retrieve user information from the AD Agent affects the amount of memory used by the feature. You specify whether the ASA uses on-demand retrieval or full download retrieval. Choosing on-demand retrieval has the benefit of using less memory, because only users of received packets are queried and stored.

## Prerequisites for the Identity Firewall

This section lists the prerequisites for configuring the Identity Firewall.

### AD Agent

- The AD Agent must be installed on a Windows server that is accessible to the ASA. Additionally, you must configure the AD Agent to obtain information from the Active Directory servers and to communicate with the ASA.

Windows 2003 R2 is not supported for the AD Agent server.

• For the steps to install and configure the AD Agent, see the Installation and Setup Guide for the Active Directory Agent.

• Before configuring the AD Agent in the ASA, obtain the secret key value that the AD Agent and the ASA use to communicate. This value must match on both the AD Agent and the ASA.

Microsoft Active Directory

• Microsoft Active Directory must be installed on a Windows server and accessible by the ASA. Supported versions include Windows 2003, 2008, and 2008 R2 servers.

• Before configuring the Active Directory server on the ASA, create a user account in Active Directory for the ASA.

• Additionally, the ASA sends encrypted log-in information to the Active Directory server by using SSL enabled over LDAP. SSL must be enabled on the Active Directory server. See the documentation for Microsoft Active Directory for how to enable SSL for Active Directory.

Before running the AD Agent Installer, you must install the patches listed in the README First for the Cisco Active Directory Agent on each Microsoft Active Directory server that the AD Agent monitors. These patches are required even when the AD Agent is installed directly on the domain controller server.

Configure the Identity Firewall

To configure the Identity Firewall, perform the following tasks:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure the Active Directory domain in the ASA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure the AD Agent in ASA.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Identity Options.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure Identity-based Security Policy.</td>
</tr>
</tbody>
</table>

Configure the Active Directory Domain

Active Directory domain configuration on the ASA is required for the ASA to download Active Directory groups and accept user identities from specific domains when receiving IP-user mapping from the AD Agent.
Before you begin

- Active Directory server IP address
- Distinguished Name for LDAP base DN
- Distinguished Name and password for the Active Directory user that the Identity Firewall uses to connect to the Active Directory domain controller

To configure the Active Directory domain, perform the following steps:

Procedure

**Step 1**
Create the AAA server group and configure AAA server parameters for the Active Directory server.

```
aaa-server server-tag protocol ldap
```

*Example:*
```
ciscoasa(config)# aaa-server adserver protocol ldap
```

**Step 2**
Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the Active Directory server.

```
aaa-server server-tag [(interface-name)] host {server-ip | name} [key] [timeout seconds]
```

*Example:*
```
ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6
```

**Step 3**
Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.

```
ldap-base-dn string
```

*Example:*
```
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com
```

Specifying the `ldap-base-dn` command is optional. If you do not specify this command, the ASA retrieves the defaultNamingContext from the Active Directory and uses it as the base DN.

**Step 4**
Specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

```
ldap-scope subtree
```

*Example:*
```
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

**Step 5**
Specify the login password for the LDAP server.

```
ldap-login-password string
```

*Example:*
```
ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword
```
Step 6 Specify the name of the directory object that the system should bind this as.

`ldap-login-dn string`

Example:

```bash
ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1
```

The ASA identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the ASA.

The `string` argument is a case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

You can specify the traditional or simplified format.

The typical `ldap-login-dn` command format includes: `CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com`.

Step 7 Configure the LDAP server model for the Microsoft Active Directory server.

`server-type microsoft`

Example:

```bash
ciscoasa(config-aaa-server-host)# server-type microsoft
```

Step 8 Specify the location of the Active Directory groups configuration in the Active Directory domain controller.

`ldap-group-base-dn string`

Example:

```bash
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com
```

If not specified, the value in the `ldap-group-base-dn` command is used. Specifying this command is optional.

Step 9 Allow the ASA to access the Active Directory domain controller over SSL.

`ldap-over-ssl enable`

Example:

```bash
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
```

To support LDAP over SSL, Active Directory server needs to be configured to have this support.

By default, the Active Directory does not have SSL configured. If SSL is not configured in the Active Directory, you do not need to configure it on the ASA for the Identity Firewall.

Step 10 Specify the server port.

`server-port port-number`

Example:

```bash
ciscoasa(config-aaa-server-host)# server-port 389
ciscoasa(config-aaa-server-host)# server-port 636
```

By default, if the `ldap-over-ssl` command is not enabled, the default server port is 389; if the `ldap-over-ssl` command is enabled, the default server port is 636.
Step 11 Set the amount of time before LDAP queries time out.

\texttt{group-search-timeout seconds}

Example:
\[\texttt{ciscoasa(config-aaa-server-host)}\# \texttt{group-search-timeout 300}\]

---

### Configure Active Directory Agents

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to the secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between the ASA and AD Agent.

**Before you begin**

- AD agent IP address
- Shared secret between the ASA and AD agent

To configure the AD Agents, perform the following steps:

**Procedure**

**Step 1** Create the AAA server group and configure AAA server parameters for the AD Agent.

\texttt{aaa-server server-tag protocol radius}

Example:
\[\texttt{ciscoasa(config)}\# \texttt{aaa-server adagent protocol radius}\]

**Step 2** Enable the AD Agent mode.

\texttt{ad-agent-mode}

Example:
\[\texttt{ciscoasa(config)}\# \texttt{ad-agent-mode}\]

**Step 3** Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the AD Agent.

\texttt{aaa-server server-tag [interface-name]] host \{server-ip | name\} [key] [timeoutseconds]}

Example:
\[\texttt{ciscoasa(config-aaa-server-group)}\# \texttt{aaa-server adagent (inside) host 192.168.1.101}\]

**Step 4** Specify the server secret value used to authenticate the ASA to the AD Agent server.

\texttt{key key}
Configure Identity Options

To configure the Identity Options for the Identity Firewall, perform the following steps:

Procedure

Step 1
Enable the Identity Firewall feature. By default, the Identity Firewall feature is disabled.

user-identity enable

Example:
ciscoasa(config)# user-identity enable

Step 2
Specify the default domain for the Identity Firewall.

user-identity default-domain domain_NetBIOS_name

Example:
ciscoasa(config)# user-identity default-domain SAMPLE

For the domain_NetBIOS_name argument, enter a name of up to 32 characters that consists of [a-z], [A-Z], [0-9], ![@#$%^&()+_=-][{}], except ‘.’ and ‘ ’ at the first character. If the domain name includes a space, enclose the entire name in quotation marks. The domain name is not case sensitive.
The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. For multiple context modes, you can set a default domain name for each context, as well as within the system execution space.

**Note**  The default domain name that you specify must match the NetBIOS domain name configured on the Active Directory domain controller. If the domain name does not match, the AD Agent incorrectly associates the user identity-IP address mapped entries with the domain name that you enter when configuring the ASA. To view the NetBIOS domain name, open the Active Directory user event security log in any text editor.

The Identity Firewall uses the LOCAL domain for all locally defined user groups or locally defined users. Users logging in through a web portal (cut-through proxy) are designated as belonging to the Active Directory domain with which they authenticated. Users logging in through a VPN are designated as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with the Active Directory. In this case, the Identity Firewall can associate the users with their Active Directory domain.

**Step 3**  Associate the LDAP parameters defined for the AAA server for importing user group queries with the domain name.

```
user-identity domain domain_nickname aaa-server aaa_server_group_tag
```

**Example:**

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

For the `domain_nickname` argument, enter a name of up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+{}[,].;] except '.' and '' at the first character. If the domain name includes a space, you must enclose that space character in quotation marks. The domain name is not case sensitive.

**Step 4**  Enable NetBIOS probing.

```
user-identity logout-probe netbios local-system probe-time minutes minutes retry-interval seconds seconds retry-count times user-not-needed [user-not-needed | match-any | exact-match]
```

**Example:**

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed
```

Enabling this option configures how often the ASA probes the user client IP address to determine whether the client is still active. By default, NetBIOS probing is disabled. To minimize the NetBIOS packets, the ASA only sends a NetBIOS probe to a client when the user has been idle for more than the specified number of minutes.

- **Exact match**—The username of the user assigned to the IP address must be the only one in the NetBIOS response. Otherwise, the user identity of that IP address is considered invalid.
- **User-not-needed**—As long as the ASA received a NetBIOS response from the client, the user identity is considered valid.

The Identity Firewall only performs NetBIOS probing for those users identities that are in the active state and exist in at least one security policy. The ASA does not perform NetBIOS probing for clients where the users logged in through cut-through proxy or by using a VPN.
Step 5  Specify the amount of time before a user is considered idle, meaning the ASA has not received traffic from the user's IP address for the specified amount of time.

user-identity inactive-user-timer minutes minutes

Example:
ciscoasa(config)# user-identity inactive-user-timer minutes 120

When the timer expires, the user's IP address is marked as inactive and removed from the local cached user identity-IP address mapping database, and the ASA no longer notifies the AD Agent about that IP address. Existing traffic is still allowed to pass. When this command is specified, the ASA runs an inactive timer even when the NetBIOS Logout Probe is configured.

By default, the idle timeout is set to 60 minutes. This option does not apply to VPN or cut-through proxy users.

Step 6  Specify the amount of time before the ASA queries the Active Directory server for user group information.

user-identity poll-import-user-group-timer hours hours

Example:
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1

If a user is added to or deleted from an Active Directory group, the ASA received the updated user group after the import group timer ran. By default, the poll-import user-group-timer hours value is 8 hours.

To immediately update user group information, enter the user-identity update import-user command.

Step 7  Specify the action when a client does not respond to a NetBIOS probe.

user-identity action netbios-response-fail remove-user-ip

Example:
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip

For example, the network connection might be blocked to that client or the client is not active.

When this command is configured, the ASA removes the user identity-IP address mapping for that client.

By default, this command is disabled.

Step 8  Specify the action when the domain is down, because the Active Directory domain controller is not responding.

user-identity action domain-controller-down domain_nickname disable-user-identity-rule

Example:
ciscoasa(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule

When the domain is down and the disable-user-identity-rule keyword is configured, the ASA disables the user identity-IP address mapping for that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the show user-identity user command.

By default, this command is disabled.

Step 9  Enable user-not-found tracking. By default, this command is disabled.

user-identity user-not-found enable
Example:

ciscoasa(config)# user-identity user-not-found enable

Only the last 1024 IP addresses are tracked.

Step 10 Specify the action when the AD Agent is not responding.

user-identity action ad-agent-down disable-user-identity-rule

Example:

ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule

When the AD Agent is down and this command is configured, the ASA disables the user identity rules associated with the users in that domain. Additionally, the status of all user IP addresses in that domain is marked as disabled in the output displayed by the show user-identity user command.

By default, this command is disabled.

Step 11 Specify the action when a user's MAC address is found to be inconsistent with the ASA IP address currently mapped to that MAC address.

user-identity actionmac-address-mismatch remove-user-ip

Example:

ciscoasa(config)# user-identity actionmac-address-mismatch remove-user-ip

When this command is configured, the ASA removes the user identity-IP address mapping for that client.

By default, the ASA uses the remove-user-ip keyword when this command is specified.

Step 12 Define how the ASA retrieves the user identity-IP address mapping information from the AD Agent.

user-identity ad-agent active-user-database {on-demand | full-download}

Example:

ciscoasa(config)# user-identity ad-agent active-user-database full-download

By default, the ASA uses the full-download option.

- **Full-download**—Specifies that the ASA send a request to the AD Agent to download the entire IP-user mapping table when the ASA starts and then to receive incremental IP-user mapping information when users log in and log out. Full downloads are event driven, meaning that when there are subsequent requests to download the database, just the updates to the user identity-IP address mapping database are sent.

- **On-demand**—Specifies that the ASA retrieve the user mapping information of an IP address from the AD Agent when the ASA receives a packet that requires a new connection, and the user of its source IP address is not in the user-identity database.

When the ASA registers a change request with the AD Agent, the AD Agent sends a new event to the ASA.

Step 13 Define the hello timer between the ASA and the AD Agent.

user-identity ad-agent hello-timer seconds seconds retry-times number

Example:

ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
The hello timer between the ASA and the AD Agent defines how frequently the ASA exchanges hello packets. The ASA uses the hello packet to obtain ASA replication status (in-sync or out-of-sync) and domain status (up or down). If the ASA does not receive a response from the AD Agent, it resends a hello packet after the specified interval.

By default, the hello timer is set to 30 seconds and 5 retries.

**Step 14**

Enable the ASA to keep track of the last event time stamp that it receives for each identifier and to discard any message if the event time stamp is at least 5 minutes older than the ASA's clock, or if its time stamp is earlier than the last event’s time stamp.

**user-identity ad-agent event-timestamp-check**

**Example:**

ciscoasa(config)# user-identity ad-agent event-timestamp-check

For a newly booted ASA that does not have knowledge of the last event time stamp, the ASA compares the event time stamp with its own clock. If the event is at least 5 minutes older, the ASA does not accept the message.

We recommend that you configure the ASA, Active Directory, and Active Directory agent to synchronize their clocks among themselves using NTP.

**Step 15**

Define the server group of the AD Agent.

**user-identity ad-agent aaa-server aaa_server_group_tag**

**Example:**

ciscoasa(config)# user-identity ad-agent aaa-server ad-agent

For the `aaa_server_group_tag` argument, enter the value defined by the `aaa-server` command.

---

**Configure Identity-Based Security Policy**

You can incorporate identity-based policy in many ASA features. Any feature that uses extended ACLs (other than those listed as unsupported in the Guidelines section) can take advantage of an identity firewall. You can now add user identity arguments to extended ACLs, as well as network-based parameters.

Features that can use identity include the following:

- **Access rules**—An access rule permits or denies traffic on an interface using network information. With an identity firewall, you can control access based on user identity.

- **AAA rules**—An authentication rule (also known as cut-through proxy) controls network access based on the user. Because this function is very similar to an access rule plus an identity firewall, AAA rules can now be used as a backup method of authentication if a user’s AD login expires. For example, for any user without a valid login, you can trigger a AAA rule. To ensure that the AAA rule is only triggered for users that do not have valid logins, you can specify special usernames in the extended ACL used for the access rule and for the AAA rule: None (users without a valid login) and Any (users with a valid login). In the access rule, configure your policy as usual for users and groups, but then include a AAA rule that permits all None users; you must permit these users so they can later trigger a AAA rule. Then, configure a AAA rule that denies Any users (these users are not subject to the AAA rule, and were handled already by the access rule), but permits all None users. For example:
For more information, see the legacy feature guide.

- Cloud Web Security—You can control which users are sent to the Cloud Web Security proxy server. In addition, you can configure policy on the Cloud Web Security ScanCenter that is based on user groups that are included in ASA traffic headers sent to Cloud Web Security.

- VPN filter—Although a VPN does not support identity firewall ACLs in general, you can configure the ASA to enforce identity-based access rules on VPN traffic. By default, VPN traffic is not subject to access rules. You can force VPN clients to abide by access rules that use an identity firewall ACL (with the `no sysopt connection permit- vão` command). You can also use an identity firewall ACL with the VPN filter feature; a VPN filter accomplishes a similar effect by allowing access rules in general.

## Collect User Statistics

To activate the collection of user statistics by the Modular Policy Framework and match lookup actions for the Identify Firewall, perform the following steps:

### Procedure

Activate the collection of user statistics by the Modular Policy Framework and matches lookup actions for the Identify Firewall.

`user-statistics [accounting | scanning]`

**Example:**

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
```

The `accounting` keyword specifies that the ASA collect the sent packet count, sent drop count, and received packet count. The `scanning` keyword specifies that the ASA collect only the sent drop count.

When you configure a policy map to collect user statistics, the ASA collects detailed statistics for selected users. When you specify the `user-statistics` command without the `accounting` or `scanning` keywords, the ASA collects both accounting and scanning statistics.
Examples for the Identity Firewall

This section provides examples for the Identity Firewall.

### AAA Rule and Access Rule Example 1

This example shows a typical cut-through proxy configuration to allow a user to log in through the ASA. In this example, the following conditions apply:

- The ASA IP address is 172.1.1.118.
- The Active Directory domain controller has the IP address 71.1.2.93.
- The end-user client has the IP address 172.1.1.118 and uses HTTPS to log in through a web portal.
- The user is authenticated by the Active Directory domain controller via LDAP.
- The ASA uses the inside interface to connect to the Active Directory domain controller on the corporate network.

``` ASA CLI
AAA Rule and Access Rule Example 1

ASA(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq 80
ASA(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq 443
ASA(config)# aaa-server LDAP protocol ldap
ASA(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ASA(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ASA(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ASA(config-aaa-server-host)# ldap-scope subtree
ASA(config-aaa-server-host)# ldap-login-dn cn=kao,OU=Employees,OU=CiscoUsers,DC=cisco,DC=com
ASA(config-aaa-server-host)# ldap-login-password *****
ASA(config-aaa-server-host)# ldap-over-ssl enable
ASA(config-aaa-server-host)# server-type microsoft
ASA(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ASA(config)#
ASA(config)# http server enable
ASA(config)# http 0.0.0.0 0.0.0.0 inside
ASA(config)#
ASA(config)# auth-prompt prompt Enter Your Authentication
ASA(config)# auth-prompt accept You are Good
ASA(config)# auth-prompt reject Goodbye
```

### AAA Rule and Access Rule Example 2

In this example, the following guidelines apply:

- In access-list commands, permit user NONE rules should be written before entering the access-list 100 ex deny any any command to allow unauthenticated incoming users to trigger AAA cut-through proxy.

- In the auth access-list command, permit user NONE rules guarantee only unauthenticated trigger cut-through proxy. Ideally, they should be the last lines.

``` ASA CLI
AAA Rule and Access Rule Example 2

ASA(config)# access-list listenerAuth extended permit tcp any any
```
VPN Filter Examples

The ASA reports users logging in through VPN authentication or a web portal (cut-through proxy) to the AD Agent, which distributes the user information to all registered ASA devices. Specifically, the IP-user mapping of authenticated users is forwarded to all ASA contexts that include the input interface where HTTP/HTTPS packets are received and authenticated. The ASA designates users logging in through a VPN as belonging the LOCAL domain.

There are two different ways to apply identity firewall rules to VPN users:

- Ensure that interface access rules, which can include identity firewall rules, are applied to VPN users.
- Bypass interface access rules, but apply a VPN filter to VPN traffic. VPN filters can include identity firewall rules.

The following topics provide examples.

Applying Interface Access Rules to VPN Traffic Example

By default, the `sysopt connection permit-vpn` command is enabled and VPN traffic is exempted from an access list check. To apply interface-based ACL rules for VPN traffic, you need to disable VPN traffic access list bypass.

In this example, if the user logs in from the outside interface, the identity firewall rules control which network resources are accessible. All VPN users are to be stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

```console
! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

Applying VPN Filters with User Specifications Example

By default, the `sysopt connection permit-vpn` command is enabled and VPN traffic is exempted from an access list check. You can use a VPN filter to apply the identity firewall rules to the VPN traffic. You can define a VPN filter with identity firewall rules in the username and group policy.

In the example, when user idfw logs in, the user can access network resources in the 10.0.00/24 subnet. However, when user user1 logs in, access to network resources in 10.0.00/24 subnet is denied. Note that all VPN users are stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

```console
! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```
Although you can use user specifications in VPN filter ACLs, the user-based rules are interpreted uni-directionally rather than bi-directionally, which is how VPN filter usually works. That is, you can filter based on user-initiated traffic, but the filter does not apply for going from the destination back to the user. For example, you could include a rule that allows a specific user to ping a server, but that rule will not allow the server to ping the user.

! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYV16IFLEsYv encrypted privilege 0
username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
group-policy group1 internal
group-policy group1 attributes
    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless

Monitoring the Identity Firewall

See the following commands for monitoring the Identity Firewall status:

- **show user-identity ad-agent**
  This command shows the status of the AD Agent and the domains.

- **show user-identity ad-agent statistics**
  This command shows the statistics for the AD Agent.

- **show user-identity memory**
  This command shows the memory usage of various modules in the Identity Firewall.

- **show user-identity user all list**
  This command shows information about all users contained in the IP-user mapping database used by the Identity Firewall.

- **show user-identity user active user domain user-name list detail**
  This command shows additional information about an active user.

- **show user-identity group**
  This command shows the list of user groups configured for the Identity Firewall.
# History for the Identity Firewall

## Table 3: History for the Identity Firewall

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Firewall</td>
<td>8.4(2)</td>
<td>The Identity Firewall feature was introduced. We introduced or modified the following commands: <code>user-identity enable</code>, <code>user-identity default-domain</code>, <code>user-identity domain</code>, <code>user-identity logout-probe</code>, <code>user-identity inactive-user-timer</code>, <code>user-identity poll-import-user-group-timer</code>, <code>user-identity action netbios-response-fail</code>, <code>user-identity user-not-found</code>, <code>user-identity action ad-agent-down</code>, <code>user-identity action mac-address-mismatch</code>, <code>user-identity action domain-controller-down</code>, <code>user-identity ad-agent active-user-database</code>, <code>user-identity ad-agent hello-timer</code>, <code>user-identity ad-agent aaa-server</code>, <code>user-identity update import-user</code>, <code>dns domain-lookup</code>, <code>dns poll-timer</code>, <code>dns expire-entry-timer</code>, <code>object-group user</code>, <code>show user-identity</code>, <code>show dns</code>, <code>clear configure user-identity</code>, <code>clear dns</code>, <code>debug user-identity</code>.</td>
</tr>
</tbody>
</table>
Chapter 6

ASA and Cisco TrustSec

This chapter describes how to implement Cisco TrustSec for the ASA.

- About Cisco TrustSec, on page 85
- Guidelines for Cisco TrustSec, on page 92
- Configure the ASA to Integrate with Cisco TrustSec, on page 95
- Example for Cisco TrustSec, on page 109
- AnyConnect VPN Support for Cisco TrustSec, on page 110
- Monitoring Cisco TrustSec, on page 111
- History for Cisco TrustSec, on page 112

About Cisco TrustSec

Traditionally, security features such as firewalls performed access control based on predefined IP addresses, subnets, and protocols. However, with enterprises transitioning to borderless networks, both the technology used to connect people and organizations and the security requirements for protecting data and networks have evolved significantly. Endpoints are becoming increasingly nomadic and users often employ a variety of endpoints (for example, laptop versus desktop, smart phone, or tablet), which means that a combination of user attributes plus endpoint attributes provide the key characteristics (in addition to existing 6-tuple based rules), that enforcement devices such as switches and routers with firewall features or dedicated firewalls can reliably use for making access control decisions.

As a result, the availability and propagation of endpoint attributes or client identity attributes have become increasingly important requirements to enable security across the customers’ networks, at the access, distribution, and core layers of the network, and in the data center.

Cisco TrustSec provides access control that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec feature, enforcement devices use a combination of user attributes and endpoint attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security across networks at the access, distribution, and core layers of the network.

Implementing Cisco TrustSec into your environment has the following advantages:

- Provides a growing mobile and complex workforce with appropriate and more secure access from any device
- Lowers security risks by providing comprehensive visibility of who and what is connecting to the wired or wireless network
• Offers exceptional control over activity of network users accessing physical or cloud-based IT resources

• Reduces total cost of ownership through centralized, highly secure access policy management and scalable enforcement mechanisms

• For more information, see the following URLs:

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>

### About SGT and SXP Support in Cisco TrustSec

In the Cisco TrustSec feature, security group access transforms a topology-aware network into a role-based network, which enables end-to-end policies enforced on the basis of role-based access control (RBAC). Device and user credentials acquired during authentication are used to classify packets by security groups. Every packet entering the Cisco TrustSec cloud is tagged with a security group tag (SGT). The tagging helps trusted intermediaries identify the source identity of the packet and enforce security policies along the data path. An SGT can indicate a privilege level across the domain when the SGT is used to define a security group ACL.

An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB), which occurs with a RADIUS vendor-specific attribute. An SGT can be assigned statically to a particular IP address or to a switch interface. An SGT is passed along dynamically to a switch or access point after successful authentication.

The Security-group eXchange Protocol (SXP) is a protocol developed for Cisco TrustSec to propagate the IP-to-SGT mapping database across network devices that do not have SGT-capable hardware support to hardware that supports SGTs and security group ACLs. SXP, a control plane protocol, passes IP-SGT mapping from authentication points (such as legacy access layer switches) to upstream devices in the network.

The SXP connections are point-to-point and use TCP as the underlying transport protocol. SXP uses the well-known TCP port number 64999 to initiate a connection. Additionally, an SXP connection is uniquely identified by the source and destination IP addresses.

### Roles in the Cisco TrustSec Feature

To provide identity and policy-based access enforcement, the Cisco TrustSec feature includes the following roles:
Access Requester (AR) — Access requesters are endpoint devices that request access to protected resources in the network. They are primary subjects of the architecture and their access privilege depends on their identity credentials.

Access requesters include endpoint devices such as PCs, laptops, mobile phones, printers, cameras, and MACsec-capable IP phones.

Policy Decision Point (PDP) — A policy decision point is responsible for making access control decisions. The PDP provides features such as 802.1x, MAB, and web authentication. The PDP supports authorization and enforcement through VLAN, DACL, and security group access (SGACL/SXP/SGT).

In the Cisco TrustSec feature, the Cisco Identity Services Engine (ISE) acts as the PDP. The Cisco ISE provides identity and access control policy functionality.

Policy Information Point (PIP) — A policy information point is a source that provides external information (for example, reputation, location, and LDAP attributes) to policy decision points.

Policy information points include devices such as Session Directory, Sensor IPS, and Communication Manager.

Policy Administration Point (PAP) — A policy administration point defines and inserts policies into the authorization system. The PAP acts as an identity repository by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping.

In the Cisco TrustSec feature, the Cisco Secure Access Control System (a policy server with integrated 802.1x and SGT support) acts as the PAP.

Policy Enforcement Point (PEP) — A policy enforcement point is the entity that carries out the decisions (policy rules and actions) made by the PDP for each AR. PEP devices learn identity information through the primary communication path that exists across networks. PEP devices learn the identity attributes of each AR from many sources, such as endpoint agents, authorization servers, peer enforcement devices, and network flows. In turn, PEP devices use SXP to propagate IP-SGT mapping to mutually trusted peer devices across the network.

Policy enforcement points include network devices such as Catalyst switches, routers, firewalls (specifically the ASA), servers, VPN devices, and SAN devices.

The Cisco ASA serves the PEP role in the identity architecture. Using SXP, the ASA learns identity information directly from authentication points and uses it to enforce identity-based policies.

Security Group Policy Enforcement

Security policy enforcement is based on security group name. An endpoint device attempts to access a resource in the data center. Compared to traditional IP-based policies configured on firewalls, identity-based policies are configured based on user and device identities. For example, mktg-contractor is allowed to access mktg-servers; mktg-corp-users are allowed to access mktg-server and corp-servers.

The benefits of this type of deployment include the following:

- User group and resource are defined and enforced using single object (SGT) simplified policy management.
- User identity and resource identity are retained throughout the Cisco TrustSec-capable switch infrastructure.

The following figure shows a deployment for security group name-based policy enforcement.
How the ASA Enforces Security Group-Based Policies

Implementing Cisco TrustSec allows you to configure security policies that support server segmentation and includes the following features:

- A pool of servers can be assigned an SGT for simplified policy management.
- The SGT information is retained within the infrastructure of Cisco TrustSec-capable switches.
- The ASA can use the IP-SGT mapping for policy enforcement across the Cisco TrustSec domain.
- Deployment simplification is possible because 802.1x authorization for servers is mandatory.

User-based security policies and security-group based policies can coexist on the ASA. Any combination of network, user-based, and security-group based attributes can be configured in a security policy.

To configure the ASA to function with Cisco TrustSec, you must import a Protected Access Credential (PAC) file from the ISE. Importing the PAC file to the ASA establishes a secure communication channel with the ISE. After the channel is established, the ASA initiates a PAC secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data (that is, the security group table). The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups.

The first time that the ASA downloads the security group table, it walks through all entries in the table and resolves all the security group names included in security policies that have been configured on it; then the ASA activates those security policies locally. If the ASA cannot resolve a security group name, it generates a syslog message for the unknown security group name.

The following figure shows how a security policy is enforced in Cisco TrustSec.
1. An endpoint device connects to an access layer device directly or via remote access and authenticates with Cisco TrustSec.

2. The access layer device authenticates the endpoint device with the ISE by using authentication methods such as 802.1X or web authentication. The endpoint device passes role and group membership information to classify the device into the appropriate security group.

3. The access layer device uses SXP to propagate the IP-SGT mapping to the upstream devices.

4. The ASA receives the packet and looks up the SGTs for the source and destination IP addresses using the IP-SGT mapping passed by SXP.
   
   If the mapping is new, the ASA records it in its local IP-SGT Manager database. The IP-SGT Manager database, which runs in the control plane, tracks IP-SGT mapping for each IPv4 or IPv6 address. The database records the source from which the mapping was learned. The peer IP address of the SXP connection is used as the source of the mapping. Multiple sources can exist for each IP-SGT mapped entry.
   
   If the ASA is configured as a Speaker, the ASA transmits all IP-SGT mapping entries to its SXP peers.

5. If a security policy is configured on the ASA with that SGT or security group name, the ASA enforces the policy. (You can create security policies on the ASA that include SGTs or security group names. To enforce policies based on security group names, the ASA needs the security group table to map security group names to SGTs.)
   
   If the ASA cannot find a security group name in the security group table and it is included in a security policy, the ASA considers the security group name to be unknown and generates a syslog message. After the ASA refreshes the security group table from the ISE and learns the security group name, the ASA generates a syslog message indicating that the security group name is known.

### Effects of Changes to Security Groups on the ISE

The ASA periodically refreshes the security group table by downloading an updated table from the ISE. Security groups can change on the ISE between downloads. These changes are not reflected on the ASA until it refreshes the security group table.
We recommend that you schedule policy configuration changes on the ISE during a maintenance window, then manually refresh the security group table on the ASA to make sure the security group changes have been incorporated.

Handling policy configuration changes in this way maximizes the chances of security group name resolution and immediate activation of security policies.

The security group table is automatically refreshed when the environment data timer expires. You can also trigger a security group table refresh on demand.

If a security group changes on the ISE, the following events occur when the ASA refreshes the security group table:

- Only security group policies that have been configured using security group names need to be resolved with the security group table. Policies that include security group tags are always active.
- When the security group table is available for the first time, all policies with security group names are walked through, security group names are resolved, and policies are activated. All policies with tags are walked through, and syslogs are generated for unknown tags.
- If the security group table has expired, policies continue to be enforced according to the most recently downloaded security group table until you clear it, or a new table becomes available.
- When a resolved security group name becomes unknown on the ASA, it deactivates the security policy; however, the security policy persists in the ASA running configuration.
- If an existing security group is deleted on the PAP, a previously known security group tag can become unknown, but no change in policy status occurs on the ASA. A previously known security group name can become unresolved, and the policy is then inactivated. If the security group name is reused, the policy is recompiled using the new tag.
- If a new security group is added on the PAP, a previously unknown security group tag can become known, a syslog message is generated, but no change in policy status occurs. A previously unknown security group name can become resolved, and associated policies are then activated.
- If a tag has been renamed on the PAP, policies that were configured using tags display the new name, and no change in policy status occurs. Policies that were configured with security group names are recompiled using the new tag value.

**Speaker and Listener Roles on the ASA**

The ASA supports SXP to send and receive IP-SGT mapping entries to and from other network devices. Using SXP allows security devices and firewalls to learn identity information from access switches without the need for hardware upgrades or changes. SXP can also be used to pass IP-SGT mapping entries from upstream devices (such as data center devices) back to downstream devices. The ASA can receive information from both upstream and downstream directions.

When configuring an SXP connection on the ASA to an SXP peer, you must designate the ASA as a Speaker or a Listener for that connection so that it can exchange Identity information:

- Speaker mode—Configures the ASA so that it can forward all active IP-SGT mapping entries collected on the ASA to upstream devices for policy enforcement.
Listener mode—Configures the ASA so that it can receive IP-SGT mapping entries from downstream devices (SGT-capable switches) and use that information to create policy definitions.

If one end of an SXP connection is configured as a Speaker, then the other end must be configured as a Listener, and vice versa. If both devices on each end of an SXP connection are configured with the same role (either both as Speakers or both as Listeners), the SXP connection fails and the ASA generates a syslog message.

Multiple SXP connections can learn IP-SGT mapping entries that have been downloaded from the IP-SGT mapping database. After an SXP connection to an SXP peer is established on the ASA, the Listener downloads the entire IP-SGT mapping database from the Speaker. All changes that occur after this are sent only when a new device appears on the network. As a result, the rate of SXP information flow is proportional to the rate at which end hosts authenticate to the network.

IP-SGT mapping entries that have been learned through SXP connections are maintained in the SXP IP-SGT mapping database. The same mapping entries may be learned through different SXP connections. The mapping database maintains one copy for each mapping entry learned. Multiple mapping entries of the same IP-SGT mapping value are identified by the peer IP address of the connection from which the mapping was learned. SXP requests that the IP-SGT Manager add a mapping entry when a new mapping is learned the first time and remove a mapping entry when the last copy in the SXP database is removed.

Whenever an SXP connection is configured as a Speaker, SXP requests that the IP-SGT Manager forward all the mapping entries collected on the device to the peer. When a new mapping is learned locally, the IP-SGT Manager requests that SXP forward it through connections that are configured as Speakers.

Configuring the ASA to be both a Speaker and a Listener for an SXP connection can cause SXP looping, which means that SXP data can be received by an SXP peer that originally transmitted it.

Register the ASA with the ISE

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can successfully import a PAC file. To register the ASA with the ISE, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log into the ISE.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Choose Administration &gt; Network Devices &gt; Network Devices.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click Add.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter the IP address of the ASA.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>When the ISE is being used for user authentication, enter a shared secret in the Authentication Settings area. When you configure the AAA server on the ASA, provide the shared secret that you create here on the ISE. The AAA server on the ASA uses this shared secret to communicate with the ISE.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specify a device name, device ID, password, and a download interval for the ASA. See the ISE documentation for how to perform these tasks.</td>
</tr>
</tbody>
</table>
Create a Security Group on the ISE

When configuring the ASA to communicate with the ISE, you specify a AAA server. When configuring the AAA server on the ASA, you must specify a server group. The security group must be configured to use the RADIUS protocol. To create a security group on the ISE, perform the following steps:

Procedure

Step 1 Log into the ISE.
Step 3 Add a security group for the ASA. (Security groups are global and not ASA specific.)
   The ISE creates an entry under Security Groups with a tag.
Step 4 In the Security Group Access area, configure device ID credentials and a password for the ASA.

Generate the PAC File

To generate the PAC file, perform the following steps.

Procedure

Step 1 Log into the ISE.
Step 2 Choose Administration > Network Resources > Network Devices.
Step 3 From the list of devices, choose the ASA.
Step 4 Under the Security Group Access (SGA), click Generate PAC.
Step 5 To encrypt the PAC file, enter a password.
   The password (or encryption key) that you enter to encrypt the PAC file is independent of the password that was configured on the ISE as part of the device credentials.
   The ISE generates the PAC file. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not have to reside on the ASA flash before you can import it.)

Guidelines for Cisco TrustSec

This section includes the guidelines and limitations that you should review before configuring Cisco TrustSec.
Failover

- You can configure security group-based policies on the ASA in both the Active/Active and Active/Standby configurations.
- When the ASA is part of a failover configuration, you must import the PAC file to the primary ASA device. You must also refresh the environment data on the primary device.
- The ASA can communicate with the ISE configured for high availability (HA).
- You can configure multiple ISE servers on the ASA and if the first server is unreachable, it continues to the next server, and so on. However, if the server list is downloaded as part of the Cisco TrustSec environment data, it is ignored.
- If the PAC file downloaded from the ISE expires on the ASA and it cannot download an updated security group table, the ASA continues to enforce security policies based on the last downloaded security group table until the ASA downloads an updated table.

Clustering

- When the ASA is part of a clustering configuration, you must import the PAC file to the master unit.
- When the ASA is part of a clustering configuration, you must refresh the environment data on the master unit.

IPv6

The ASA supports SXP for IPv6 and IPv6-capable network devices. The AAA server must use an IPv4 address.

Layer 2 SGT Imposition

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI.
- Does not support link encryption using SAP negotiation and MACsec.
- Not supported on failover links.
- Not supported on cluster control links.
- The ASA does not reclassify existing flows if the SGT is changed. Any policy decisions that were made based on the previous SGT remain in force for the life of the flow. However, the ASA can immediately reflect SGT changes on egress packets, even if the packets belong to a flow whose classification was based on a previous SGT.
- The hardware architecture of the ASA 5585-X is designed to load balance regular packets in an optimal way, but this is not the case for inline tagged packets with Layer 2 Security Group Tagging Imposition. Significant performance degradation on the ASA 5585-X may occur when it processes incoming inline tagged packets. This issue does not occur with inline tagged packets on other ASA platforms, as well as with untagged packets on the ASA 5585-X. One workaround is to offload access policies so that minimal inline tagged packets go to the ASA 5585-X, which allows the switches to handle tagged policy enforcement. Another workaround is to use SXP so that the ASA 5585-X can map the IP address to the security group tag without the need to receive tagged packets.
• The ASASM does not support Layer 2 Security Group Tagging Imposition.

Additional Guidelines

• The ASA supports SXP Version 3. The ASA negotiates SXP versions with different SXP-capable network devices.

• You can configure the ASA to refresh the security group table when the SXP reconcile timer expires and you can download the security group table on demand. When the security group table on the ASA is updated from the ISE, changes are reflected in the appropriate security policies.

• Cisco TrustSec supports the Smart Call Home feature in single context and multi-context mode, but not in the system context.

• The ASA can only be configured to interoperate in a single Cisco TrustSec domain.

• The ASA does not support static configuration of SGT-name mapping on the device.

• NAT is not supported in SXP messages.

• SXP conveys IP-SGT mapping to enforcement points in the network. If an access layer switch belongs to a different NAT domain than the enforcing point, the IP-SGT map that it uploads is invalid, and an IP-SGT mapping database lookup on the enforcement device does not yield valid results. As a result, the ASA cannot apply security group-aware security policy on the enforcement device.

• You can configure a default password for the ASA to use for SXP connections, or you can choose not to use a password; however, connection-specific passwords are not supported for SXP peers. The configured default SXP password should be consistent across the deployment network. If you configure a connection-specific password, connections may fail and a warning message appears. If you configure the connection with the default password, but it is not configured, the result is the same as when you have configured the connection with no password.

• The ASA can be configured as an SXP Speaker or Listener, or both. However, SXP connection loops can form when a device has bidirectional connections to a peer or is part of a unidirectionally connected chain of devices. (The ASA can learn IP-SGT mapping for resources from the access layer in the data center. The ASA might need to propagate these tags to downstream devices.) SXP connection loops can cause unexpected behavior of SXP message transport. In cases where the ASA is configured to be a Speaker and Listener, an SXP connection loop can occur, causing SXP data to be received by the peer that originally transmitted it.

• When changing the ASA local IP address, you must ensure that all SXP peers have updated their peer list. In addition, if SXP peers changes its IP addresses, you must ensure those changes are reflected on the ASA.

• Automatic PAC file provisioning is not supported. The ASA administrator must request the PAC file from the ISE administrative interface and import it into the ASA.

• PAC files have expiration dates. You must import the updated PAC file before the current PAC file expires; otherwise, the ASA cannot retrieve environment data updates. If the PAC file downloaded from the ISE expires on the ASA and it cannot download an updated security group table, the ASA continues to enforce security policies based on the last downloaded security group table until the ASA downloads an updated table.

• When a security group changes on the ISE (for example, it is renamed or deleted), the ASA does not change the status of any ASA security policies that contain an SGT or security group name associated
with the changed security group; however, the ASA generates a syslog message to indicate that those
security policies changed.

- The multi-cast types are not supported in ISE 1.0.
- An SXP connection stays in the initializing state among two SXP peers interconnected by the ASA; as
  shown in the following example:

  (SXP peer A) - - - - (ASA) - - - (SXP peer B)

Therefore, when configuring the ASA to integrate with Cisco TrustSec, you must enable the no-NAT,
no-SEQ-RAND, and MD5-AUTHENTICATION TCP options on the ASA to configure SXP connections.
Create a TCP state bypass policy for traffic destined to SXP port TCP 64999 among the SXP peers. Then
apply the policy on the appropriate interfaces.

For example, the following set of commands shows how to configure the ASA for a TCP state bypass
policy:

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
  tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
  match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512

policy-map global_policy
  class SXP-MD5-CLASSMAP
    set connection random-sequence-number disable
    set connection advanced-options SXP-MD5-OPTION-ALLOW
    set connection advanced-options tcp-state-bypass

service-policy global_policy global
```

### Configure the ASA to Integrate with Cisco Trustsec

To configure the ASA to integrate with Cisco TrustSec, perform the following tasks.

**Before you begin**

Before configuring the ASA to integrate with Cisco TrustSec, you must complete the following tasks in ISE:

- Register the ASA with the ISE, on page 91
- Create a Security Group on the ISE, on page 92
- Generate the PAC File, on page 92
Configure the AAA Server for Cisco TrustSec Integration

This section describes how to integrate the AAA server for Cisco TrustSec. To configure the AAA server group to communicate with the ISE on the ASA, perform the following steps.

Before you begin

- The referenced server group must be configured to use the RADIUS protocol. If you add a non-RADIUS server group to the ASA, the configuration fails.
- If the ISE is also used for user authentication, obtain the shared secret that was entered on the ISE when you registered the ASA with the ISE. Contact your ISE administrator to obtain this information.

Procedure

Step 1  Create the AAA server group and configure the AAA server parameters for the ASA to communicate with the ISE server.

```
aaa-server server-tag protocol radius
```

Example:

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

The `server-tag` argument specifies the server group name.

Step 2  Exit from the aaa server group configuration mode.

```
exit
```

Example:

```
ciscoasa(config-aaa-server-group)# exit
```
Step 3 Configure a AAA server as part of a AAA server group and set host-specific connection data.

ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip

Example:

ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1

The interface-name argument specifies the network interface where the ISE server resides. The parentheses are required in this parameter. The server-tag argument is the name of the AAA server group. The server-ip argument specifies the IP address of the ISE server.

Step 4 Specify the server secret value used to authenticate the ASA with the ISE server.

key key

Example:

ciscoasa(config-aaa-server-host)# key myexclusivekey

The key argument is an alphanumeric keyword up to 127 characters long.

If the ISE is also used for user authentication, enter the shared secret that was entered on the ISE when you registered the ASA with the ISE.

Step 5 Exit from the aaa server host configuration mode.

exit

Example:

ciscoasa(config-aaa-server-host)# exit

Step 6 Identify the AAA server group that is used by Cisco TrustSec for environment data retrieval.

cs server-group AAA-server-group-name

Example:

ciscoasa(config)# cts server-group ISEserver

The AAA-server-group-name argument is the name of the AAA server group that you specified in Step 1 in the server-tag argument.

Note You may configure only one instance of the server group on the ASA for Cisco TrustSec.

The following example shows how to configure the ASA to communicate with the ISE server for Cisco TrustSec integration:

ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivekey

ciscoasa(config-aaa-server-host)# exit
Import a PAC File

This section describes how to import a PAC file.

Before you begin

- The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can generate a PAC file.
- Obtain the password used to encrypt the PAC file when generating it on the ISE. The ASA requires this password to import and decrypt the PAC file.
- The ASA requires access to the PAC file generated by the ISE. The ASA can import the PAC file from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC file does not need to reside on the ASA flash before you can import it.)
- The server group has been configured for the ASA.

To import a PAC file, perform the following steps:

Procedure

Import a Cisco TrustSec PAC file.

```
ciscoasa(config)# cts import-pac filepath password value
```

Example:

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

The `value` argument specifies the password used to encrypt the PAC file. The password is independent of the password that was configured on the ISE as part of the device credentials. The `filepath` argument is entered as one of the following options:

**Single Mode**

- `disk0`: Path and filename on disk0
- `disk1`: Path and filename on disk1
- `flash`: Path and filename on flash
- `ftp`: Path and filename on FTP
- `http`: Path and filename on HTTP
- `https`: Path and filename on HTTPS
- `smb`: Path and filename on SMB
- `tftp`: Path and filename on TFTP
Configure the Security Exchange Protocol

You need to enable and configure the Security Exchange Protocol (SXP) to use Cisco Trustsec.

Before you begin

At least one interface must be in the UP/UP state. If you enable SXP with all interfaces down, the ASA does not display a message indicating that SXP is not working or it could not be enabled. If you check the

Configure the Security Exchange Protocol

You need to enable and configure the Security Exchange Protocol (SXP) to use Cisco Trustsec.

Before you begin

At least one interface must be in the UP/UP state. If you enable SXP with all interfaces down, the ASA does not display a message indicating that SXP is not working or it could not be enabled. If you check the
configuration by entering the `show running-config` command, the command output displays the following message:

“WARNING: SXP configuration in process, please wait for a few moments and try again.”

**Procedure**

**Step 1**
Enable SXP on the ASA. By default, SXP is disabled.

`cts sxp enable`

**Example:**

```
ciscoasa(config)# cts sxp enable
```

**Step 2**
(Optional; not recommended.) Configure the default source IP address for SXP connections.

`cts sxp default source-ip ipaddress`

**Example:**

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

The `ipaddress` argument is an IPv4 or IPv6 address.

When you configure a default source IP address for SXP connections, you must specify the same address as the ASA outbound interface. If the source IP address does not match the address of the outbound interface, SXP connections fail.

When a source IP address for an SXP connection is not configured, the ASA performs a route/ARP lookup to determine the outbound interface for the SXP connection. We recommend that you do not configure a default source IP address for SXP connections and allow the ASA to perform a route/ARP lookup to determine the source IP address for an SXP connection.

**Step 3**
(Optional.) Configure the default password for TCP MD5 authentication with SXP peers. By default, SXP connections do not have a password.

`cts sxp default password [0 | 8] password`

**Example:**

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

Configure a default password if and only if you configure the SXP connection peers to use the default password. The length of the password depends on the decryption level, which defaults to 0 if you do not specify it:

- **0**—Unencrypted cleartext. The password can be up to 80 characters.
- **8**—Encrypted text. The password can be up to 162 characters.

**Step 4**
(Optional.) Specify the time interval between ASA attempts to set up new SXP connections between SXP peers.
**cts sxp retry period** \textit{timervalue}

\textbf{Example:}

ciscoasa(config)# cts sxp retry period 60

The ASA continues to make connection attempts until a successful connection is made, waiting the retry interval before trying again after a failed attempt. You can specify a retry period from 0 to 64000 seconds. The default is 120 seconds. If you specify 0 seconds, the ASA does not try to connect to SXP peers.

We recommend that you configure the retry timer to a different value from its SXP peer devices.

**Step 5**

(Optional.) Specify the value of the reconciliation timer.

**cts sxp reconciliation period** \textit{timervalue}

\textbf{Example:}

ciscoasa(config)# cts sxp reconciliation period 60

After an SXP peer terminates its SXP connection, the ASA starts a hold down timer. If an SXP peer connects while the hold down timer is running, the ASA starts the reconciliation timer; then, the ASA updates the SXP mapping database to learn the latest mappings.

When the reconciliation timer expires, the ASA scans the SXP mapping database to identify stale mapping entries (which were learned in a previous connection session). The ASA marks these connections as obsolete. When the reconciliation timer expires, the ASA removes the obsolete entries from the SXP mapping database.

You can specify a reconciliation period from 1 to 64000 seconds. The default is 120 seconds.

**Step 6**

(Optional.) Configure the delete-hold-down timer for the IP-SGT mappings learned from a peer after an SXP peer terminates its SXP connection.

**cts sxp delete-hold-down period** \textit{timervalue}

The timer value specifies the number of seconds, 120-64000, that IP-SGT mappings learned from a torn-down SXP connection are held before being deleted.

\textbf{Example:}

ciscoasa(config)# cts sxp delete-hold-down period 240

Each SXP connection is associated with a delete hold down timer. This timer is triggered when an SXP connection on the listener side is torn down. The IP-SGT mappings learned from this SXP connection are not deleted immediately. Instead, they are held until the delete hold down timer expires. The mappings are deleted upon the expiry of this timer.

**Step 7**

(Optional.) Configure the depth of IPv4 subnet expansion when acting as a speaker to peers that use SXPv2 or lower.

**cts sxp mapping network-map** \textit{maximum_hosts}

If a peer uses SXPv2 or lower, the peer cannot understand SGT to subnet bindings. The ASA can expand the IPv4 subnet bindings to individual host bindings (IPv6 bindings are not expanded). This command specifies the maximum number of host bindings that can be generated from a subnet binding.
You can specify the maximum number to be from 0 to 65535. The default is 0, which means that subnet bindings are not expanded to host bindings.

---

### Add an SXP Connection Peer

To add an SXP connection peer, perform the following steps:

**Procedure**

Set up an SXP connection to an SXP peer.

```plaintext
cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}
```

**Example:**

```plaintext
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP connections are set per IP address; a single device pair can service multiple SXP connections.

The `peer_ip_address` argument is the IPv4 or IPv6 address of the SXP peer. The peer IP address must be reachable from the ASA outgoing interface.

The `source_ip_address` argument is the local IPv4 or IPv6 address of the SXP connection. The source IP address must be the same as the ASA outbound interface or the connection fails.

We recommend that you do not configure a source IP address for an SXP connection and allow the ASA to perform a route/ARP lookup to determine the source IP address for the SXP connection.

Indicate whether or not to use the authentication key for the SXP connection:

- **default**—Use the default password configured for SXP connections.
- **none**—Do not use a password for the SXP connection.

Indicate the mode of the SXP connection:

- **local**—Use the local SXP device.
- **peer**—Use the peer SXP device.

Indicate whether the ASA functions as a Speaker or Listener for the SXP connection.

- **speaker**—The ASA can forward IP-SGT mapping to upstream devices.
- **listener**—The ASA can receive IP-SGT mapping from downstream devices.

The following example shows how to configure SXP peers on the ASA:

```plaintext
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
```
Refresh Environment Data

The ASA downloads environment data from the ISE, which includes the Security Group Tag (SGT) name table. The ASA automatically refreshes its environment data that is obtained from the ISE when you complete the following tasks on the ASA:

- Configure a AAA server to communicate with the ISE.
- Import a PAC file from the ISE.
- Identify the AAA server group that the ASA will use to retrieve Cisco TrustSec environment data.

Normally, you do not need to manually refresh the environment data from the ISE; however, security groups can change on the ISE. These changes are not reflected on the ASA until you refresh the data in the ASA security group table, so refresh the data on the ASA to make sure that any security group changes made on the ISE are reflected on the ASA.

We recommend that you schedule policy configuration changes on the ISE and the manual data refresh on the ASA during a maintenance window. Handling policy configuration changes in this way maximizes the chances of security group names getting resolved and security policies becoming active immediately on the ASA.

To refresh the environment data, perform the following steps:

**Procedure**

Refresh the environment data from the ISE and reset the reconcile timer to the configured default value.

```
cts refresh environment-data
```

**Example:**

```
ciscoasa(config)# cts refresh environment-data
```

Configure the Security Policy

You can incorporate Cisco TrustSec policy in many ASA features. Any feature that uses extended ACLs (unless listed in this chapter as unsupported) can take advantage of Cisco TrustSec. You can add security group arguments to extended ACLs, as well as traditional network-based parameters.

- To configure an extended ACL, see Add an Extended ACE for Security Group-Based Matching (Cisco TrustSec), on page 32.
• To configure security group object groups that can be used in the ACL, see Configure Security Group Object Groups, on page 16.

For example, an access rule permits or denies traffic on an interface using network information. With Cisco TrustSec, you can control access based on security group. For example, you could create an access rule for sample_securitygroup1 10.0.0.0 255.0.0.0, meaning the security group could have any IP address on subnet 10.0.0.0/8.

You can configure security policies based on combinations of security group names (servers, users, unmanaged devices, and so on), user-based attributes, and traditional IP-address-based objects (IP address, Active Directory object, and FQDN). Security group membership can extend beyond roles to include device and location attributes and is independent of user group membership.

The following example shows how to create an ACL that uses a locally defined security object group:

object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name // single sg_name
   group-object it-admin // locally defined object-group as nested object
object-group security objgrp-hr-network
object-group security objgrp-hr-servers
security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
object-group-security objgrp-hr-network

The ACL configured in the previous example can be activated by configuring an access group or the Modular Policy Framework.

Additional examples:

!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group-name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSCO\mary any security-group name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
to dst objgrp-hr-network any network
access-list idfw-acl permit ip user CSCO\Jack object-group-security objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google
Configure Layer 2 Security Group Tagging Imposition

Cisco TrustSec identifies and authenticates each network user and resource and assigns a 16-bit number called a Security Group Tag (SGT). This identifier is in turn propagated between network hops, which allows any intermediary devices such as ASAs, switches, and routers to enforce polices based on this identity tag.

SGT plus Ethernet Tagging, also called Layer 2 SGT Imposition, enables the ASA to send and receive security group tags on Ethernet interfaces using Cisco proprietary Ethernet framing (EtherType 0x8909), which allows the insertion of source security group tags into plain-text Ethernet frames. The ASA inserts security group tags on the outgoing packet and processes security group tags on the incoming packet, based on a manual per-interface configuration. This feature allows inline hop-by-hop propagation of endpoint identity across network devices and provides seamless Layer 2 SGT Imposition between each hop.

The following figure shows a typical example of Layer 2 SGT Imposition.

**Figure 12: Layer 2 SGT Imposition**

Usage Scenarios

The following table describes the expected behavior for ingress traffic when configuring this feature.
### Table 4: Ingress Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged Packet Received</th>
<th>Untagged Packet Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued.</td>
<td>Packet is dropped.</td>
<td>SGT value is from the IP-SGT Manager.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued.</td>
<td>SGT value is from the IP-SGT Manager.</td>
<td>SGT value is from the IP-SGT Manager.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>policy static sgt sgt_number</code> command are both issued.</td>
<td>SGT value is from the <code>policy static sgt sgt_number</code> command.</td>
<td>SGT value is from the <code>policy static sgt sgt_number</code> command.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>policy static sgt sgt_number trusted</code> command are both issued.</td>
<td>SGT value is from the inline SGT in the packet.</td>
<td>SGT value is from the <code>policy static sgt sgt_number</code> command.</td>
</tr>
</tbody>
</table>

If there is no matched IP-SGT mapping from the IP-SGT Manager, then a reserved SGT value of “0x0” for “Unknown” is used.

The following table describes the expected behavior for egress traffic when configuring this feature.

### Table 5: Egress Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged or Untagged Packet Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued.</td>
<td>Untagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued.</td>
<td>Tagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>propagate sgt</code> command are both issued.</td>
<td>Tagged</td>
</tr>
<tr>
<td>The <code>cts manual</code> command and the <code>no propagate sgt</code> command are both issued.</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

The following table describes the expected behavior for to-the-box and from-the-box traffic when configuring this feature.

### Table 6: To-the-box and From-the-box Traffic

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Tagged or Untagged Packet Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>No command is issued on the ingress interface for to-the-box traffic.</td>
<td>Packet is dropped.</td>
</tr>
<tr>
<td>The <code>cts manual</code> command is issued on the ingress interface for to-the-box traffic.</td>
<td>Packet is accepted, but there is no policy enforcement or SGT propagation.</td>
</tr>
</tbody>
</table>
### Configure a Security Group Tag on an Interface

To configure a security group tag on an interface, perform the following steps:

**Procedure**

**Step 1**
Specify an interface and enter interface configuration mode.

```plaintext
interface id
```

**Example:**

```
ciscoasa(config)# interface gigabitethernet 0/0
```

**Step 2**
Enable Layer 2 SGT Imposition and enter cts manual interface configuration mode.

```plaintext
cts manual
```

**Example:**

```
ciscoasa(config-if)# cts manual
```

**Step 3**
Enable propagation of a security group tag on an interface. Propagation is enabled by default.

```plaintext
propagate sgt
```

**Example:**

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

**Step 4**
Apply a policy to a manually configured CTS link.

```plaintext
policy static sgt sgt_number [trusted]
```

**Example:**

```
ciscoasa(config-if-cts-manual)# policy static sgt 0 trusted
```
The `static` keyword specifies an SGT policy to incoming traffic on the link. The `sgt_number` keyword-argument pair specifies the SGT number to apply to incoming traffic from the peer. Valid values are from 2-65519.

The `trusted` keyword indicates that ingress traffic on the interface with the SGT specified in the command should not have its SGT overwritten. Untrusted is the default.

The following example enables an interface for Layer 2 SGT imposition and defines whether or not the interface is trusted:

```bash
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

**Configure IP-SGT Bindings Manually**

To configure IP-SGT bindings manually, perform the following steps:

**Procedure**

Configure IP-SGT bindings manually.

**Example:**

```bash
ciscoasa(config)# cts role-based sgt-map IPv4_addr IPv6_addr[\mask] [\prefix] sgt sgt_value
```

You can specify an IPv4 or IPv6 host address. You can also specify network addresses by including a subnet mask or prefix value (for IPv6), such as 10.100.10.0/24. The `sgt_value` is the SGT number, from 2 to 65519.

**Troubleshooting Tips**

Use the `packet-tracer` command to determine why a particular session was allowed or denied, which SGT value is being used (from the SGT in the packet, from the IP-SGT manager, or from the `policy static sgt` command configured on the interface), and which security group-based security policies were applied.

The following example displays output from the `packet-tracer` command to show security group tag mapping to an IP address:

```bash
ciscoasa# packet-tracer input inside tcp inline-tag 100
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------

Use the `capture capture-name type inline-tag tag` command to capture only the Cisco CMD packets (EtherType 0x8909) with or without a specific SGT value.

The following example displays output from the `show capture` command for a specified SGT value:

ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply

**Example for Cisco TrustSec**

The following example shows how to configure the ASA to use Cisco TrustSec:

```bash
// Import an encrypted CTS PAC file
csimport-pac asapac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cs server-group cts-server-list
// Configure SXP peers
cs exp enable
cs exp connection peer 192.168.1.100 password default mode peer speaker
// Configure security-group based policies
object-group security objgrp-it-admin
security-group name it-admin-sg-name
security-group tag 1
object-group security objgrp-hr-admin
security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
// Configure security group tagging plus Ethernet tagging
interface gi0/1
cts manual
propagate sgt
policy static sgt 100 trusted
cs role-based sgt-map 10.1.1.100 sgt 50
```

**CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10**
AnyConnect VPN Support for Cisco TrustSec

ASA supports security group tagging of VPN sessions. You can assign a Security Group Tag (SGT) to a VPN session using an external AAA server, or by configuring a security group tag for a local user or for a VPN group policy. This tag can then be propagated through the Cisco TrustSec system over Layer 2 Ethernet. Security group tags are useful on group policies and for local users when the AAA server cannot provide an SGT.

Following is the typical process for assigning an SGT to a VPN user:

1. A user connects to a remote access VPN that uses a AAA server group containing ISE servers.
2. The ASA requests AAA information from ISE, which might include an SGT. The ASA also assigns an IP address for the user’s tunneled traffic.
3. The ASA uses AAA information to authenticate the user and creates a tunnel.
4. The ASA uses the SGT from AAA information and the assigned IP address to add an SGT in the Layer 2 header.
5. Packets that include the SGT are passed to the next peer device in the Cisco TrustSec network.

If there is no SGT in the attributes from the AAA server to assign to a VPN user, then the ASA uses the SGT in the group policy. If there is no SGT in the group policy, then tag 0x0 is assigned.

Note

You can also use ISE for policy enforcement using ISE Change of Authorization (CoA). For information on how to configure policy enforcement, see the VPN configuration guide.

Add an SGT to Remote Access VPN Group Policies and Local Users

To configure an SGT attribute on remote access VPN group policies, or on the VPN policy for a user defined in the LOCAL user database, perform the following steps.

There is no default SGT for group policies or local users.

Procedure

Step 1

To configure an SGT on a remote access VPN group policy:

a) Enter group-policy configuration mode:

   group-policy name

   Example:

   ciscoasa(config)# group policy Gpolicy1

b) Configure the SGT for the group policy.

   security-group-tag {none | value sgt}
If you set a tag using value, the tag can be from 2 to 65519. Specify none to set no SGT.

Example:

ciscoasa(config-group-policy)# security-group-tag value 101

Step 2  To configure an SGT on for a user in the LOCAL database:

a) If necessary, create the user.

username name {nopassword | password password [encrypted]} [privilege priv_level]

Example:

ciscoasa(config)# username newuser password changeme encrypted privilege 15

b) Enter username configuration mode.

username name attributes

Example:

asa3(config)# username newuser attributes
asa3(config-username)#

c) Configure the SGT for the user.

security-group-tag {none | value sgt}

If you set a tag using value, the tag can be from 2 to 65519. Specify none to set no SGT.

Example:

ciscoasa(config-username)# security-group-tag value 101

Monitoring Cisco TrustSec

See the following commands for monitoring Cisco TrustSec:

- show running-config cts
- show running-config [all] cts role-based [sgt-map]
  This command shows the user-defined IP-SGT binding table entries.
- show cts sxp connections
  This command shows the SXP connections on the ASA for a particular user context when multiple context mode is used.
- show conn security-group
  Shows data for all SXP connections.
- **show cts environment-data**
  Shows the Cisco TrustSec environment information contained in the security group table on the ASA.

- **show cts sgt-map**
  Shows the IP address-security group table manager entries in the control path.

- **show asp table cts sgt-map**
  This command shows the IP address-security group table mapping entries from the IP address-security group table mapping database maintained in the datapath.

- **show cts pac**
  Shows information about the PAC file imported into the ASA from the ISE and includes a warning message when the PAC file has expired or is within 30 days of expiration.

## History for Cisco TrustSec

### Table 7: History for Cisco TrustSec

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco TrustSec | 9.0(1)            | Cisco TrustSec provides access control that builds on an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec feature, enforcement devices use a combination of user attributes and endpoint attributes to make role-based and identity-based access control decisions.

In this release, the ASA integrates with Cisco TrustSec to provide security group-based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses.

The ASA can use Cisco TrustSec for other types of security group-based policies, such as application inspection; for example, you can configure a class map that includes an access policy based on a security group.

We introduced or modified the following commands: **access-list extended, cts sxp enable, cts server-group, cts sxp default, cts sxp retry period, cts sxp reconciliation period, cts sxp connection peer, cts import-pac, cts refresh environment-data, object-group security, security-group, show running-config cts, show running-config object-group, clear configure cts, clear configure object-group, show cts pac, show cts environment-data, show cts environment-data sg-table, show cts sxp connections, show object-group, show configure security-group, clear cts environment-data, debug cts, and packet-tracer.**
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Security Group Tag Imposition</td>
<td>9.3(1)</td>
<td>You can now use security group tagging combined with Ethernet tagging to enforce policies. SGT plus Ethernet Tagging, also called Layer 2 SGT Imposition, enables the ASA to send and receive security group tags on Ethernet interfaces using Cisco proprietary Ethernet framing (EtherType 0x8909), which allows the insertion of source security group tags into plain-text Ethernet frames. We introduced or modified the following commands: <code>cts manual</code>, <code>policy static sgt</code>, <code>propagate sgt</code>, <code>cts role-based sgt-map</code>, <code>show cts sgt-map</code>, <code>packet-tracer</code>, <code>capture</code>, <code>show capture</code>, <code>show asp drop</code>, <code>show asp table classify</code>, <code>show running-config all</code>, <code>clear configure all</code>, and <code>write memory</code>.</td>
</tr>
<tr>
<td>Cisco Trustsec support for Security Exchange Protocol (SXP) version 3.</td>
<td>9.6(1)</td>
<td>Cisco Trustsec on ASA now implements SXPv3, which enables SGT-to-subnet bindings, which are more efficient than host bindings. We introduced or modified the following commands: <code>cts sxp mapping network-map</code>, <code>cts role-based sgt-map</code>, <code>show cts sgt-map</code>, <code>show cts sxp sgt-map</code>, <code>show asp table cts sgt-map</code>.</td>
</tr>
<tr>
<td>Trustsec SXP connection configurable delete hold down timer</td>
<td>9.8(3)</td>
<td>The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds. New/Modified commands: <code>cts sxp delete-hold-down period</code>, <code>show cts sxp connection brief</code>, <code>show cts sxp connections</code></td>
</tr>
</tbody>
</table>
ASA FirePOWER Module

The following topics describe how to configure the ASA FirePOWER module that runs on the ASA.

- About the ASA FirePOWER Module, on page 115
- Licensing Requirements for the ASA FirePOWER Module, on page 119
- Guidelines for ASA FirePOWER, on page 119
- Defaults for ASA FirePOWER, on page 121
- Perform Initial ASA FirePOWER Setup, on page 121
- Configure the ASA FirePOWER Module, on page 130
- Managing the ASA FirePOWER Module, on page 134
- Monitoring the ASA FirePOWER Module, on page 142
- Examples for the ASA FirePOWER Module, on page 145
- History for the ASA FirePOWER Module, on page 146

About the ASA FirePOWER Module

The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

The ASA FirePOWER module runs a separate application from the ASA. The module can be a hardware module (on the ASA 5585-X only) or a software module (all other models).

How the ASA FirePOWER Module Works with the ASA

You can configure your ASA FirePOWER module using one of the following deployment models:

- Inline mode—In an inline deployment, the actual traffic is sent to the ASA FirePOWER module, and the module’s policy affects what happens to the traffic. After dropping undesired traffic and taking any other actions applied by policy, the traffic is returned to the ASA for further processing and ultimate transmission.

- Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.
• Passive monitor-only (traffic forwarding) mode—If you want to prevent any possibility of the ASA with FirePOWER Services device impacting traffic, you can configure a traffic-forwarding interface and connect it to a SPAN port on a switch. In this mode, traffic is sent directly to the ASA FirePOWER module without ASA processing. The traffic is “black holed,” in that nothing is returned from the module, nor does the ASA send the traffic out any interface. You must operate the ASA in single context transparent mode to configure traffic forwarding.

Be sure to configure consistent policies on the ASA and the ASA FirePOWER. Both policies should reflect the inline or monitor-only mode of the traffic.

The following sections explain these modes in more detail.

ASA FirePOWER Inline Mode

In inline mode, traffic goes through the firewall checks before being forwarded to the ASA FirePOWER module. When you identify traffic for ASA FirePOWER inspection on the ASA, traffic flows through the ASA and the module as follows:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA FirePOWER module.
5. The ASA FirePOWER module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA FirePOWER module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

The following figure shows the traffic flow when using the ASA FirePOWER module in inline mode. In this example, the module blocks traffic that is not allowed for a certain application. All other traffic is forwarded through the ASA.

Figure 13: ASA FirePOWER Module Traffic Flow in the ASA
If you have a connection between hosts on two ASA interfaces, and the ASA FirePOWER service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA FirePOWER module, including traffic originating on the non-ASA FirePOWER interface (because the feature is bidirectional).

ASA FirePOWER Inline Tap Monitor-Only Mode

This mode sends a duplicate stream of traffic to the ASA FirePOWER module for monitoring purposes only. The module applies the security policy to the traffic and lets you know what it would have done if it were operating in inline mode; for example, traffic might be marked “would have dropped” in events. You can use this information for traffic analysis and to help you decide if inline mode is desirable.

ASA FirePOWER Passive Monitor-Only Traffic Forwarding Mode

If you want to operate the ASA FirePOWER module as a pure Intrusion Detection System (IDS), where there is no impact on the traffic at all, you can configure a traffic forwarding interface. A traffic forwarding interface sends all received traffic directly to the ASA FirePOWER module without any ASA processing.

The module applies the security policy to the traffic and lets you know what it would have done if it were operating in inline mode; for example, traffic might be marked “would have dropped” in events. You can use this information for traffic analysis and to help you decide if inline mode is desirable.

Traffic in this setup is never forwarded: neither the module nor the ASA sends the traffic on to its ultimate destination. You must operate the ASA in single context and transparent modes to use this configuration.

The following figure shows an interface configured for traffic-forwarding. That interface is connected to a switch SPAN port so the ASA FirePOWER module can inspect all of the network traffic. Another interface sends traffic normally through the firewall.
ASA FirePOWER Management

The module has a basic command line interface (CLI) for initial configuration and troubleshooting only. You configure the security policy on the ASA FirePOWER module using one of the following methods:

- Firepower/FireSIGHT Management Center—Can be hosted on a separate Management Center appliance or as a virtual appliance. The Management Center application is called Firepower beginning in version 6.0. Previous versions are called FireSIGHT.

- ASDM (check for compatibility with your model/version)—You can manage both the ASA and the module using the on-box ASDM.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA FirePOWER module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

You must follow these configuration restrictions on the ASA:

- Do not configure ASA inspection on HTTP traffic that you send to the ASA FirePOWER module.

- Do not configure Cloud Web Security (ScanSafe) inspection on traffic that you send to the ASA FirePOWER module. If traffic matches both your Cloud Web Security and ASA FirePOWER service policies, the traffic is forwarded to the ASA FirePOWER module only. If you want to implement both services, ensure there is no overlap between the traffic matching criteria for each service.

- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA FirePOWER module.

Other application inspections on the ASA are compatible with the ASA FirePOWER module, including the default inspections.
What to Do if the ASA FirePOWER Module Cannot Filter URLs

The ASA FirePOWER module obtains its URL filtering data from the managing Firepower Management Center, over HTTP. The module cannot perform URL filtering if it cannot download this database.

If there is a device between the ASA FirePOWER module and Firepower Management Center that is performing ASA HTTP inspection, or HTTP inspection using an ASA CX module, the inspections can block the ASA FirePOWER module's HTTP GET requests to the Firepower Management Center. This problem also occurs if you configure HTTP inspection on the ASA that hosts the ASA FirePOWER module (which is a misconfiguration).

To resolve the issues, do any of the following that apply to your situation:

- If you configured HTTP inspection on the ASA that hosts the ASA FirePOWER module, remove the HTTP inspection configuration. ASA FirePOWER inspection and ASA HTTP inspection are incompatible.

- If there is an intervening device doing ASA HTTP inspection, remove the drop protocol violations action from the HTTP inspection policy map:

  ```
  policy-map type inspect http http_inspection_policy
  parameters
  no protocol-violation action drop-connection
  ```

- If there is an intervening ASA CX module, bypass the CX module for connections between the ASA FirePOWER module and the Firepower Management Center's management IP address.

Licensing Requirements for the ASA FirePOWER Module

Certain areas of ASA FirePOWER module functionality may require additional licenses.

For an ASA FirePOWER module managed by a Firepower/FireSIGHT Management Center, enable licenses on the module using the Management Center. See the licensing chapter of the FireSIGHT System User Guide 5.4, Firepower Management Center Configuration Guide 6.0, or the online help on the FireSIGHT Management Center for more information.

For the ASA FirePOWER module managed using ASDM, enable licenses on the module using the FirePOWER module configuration in ASDM. See the licensing chapter of the ASA FirePOWER Module User Guide 5.4, ASA FirePOWER Services Local Management Configuration Guide 6.0, or the online help for the module in ASDM for more information.

The ASA itself does not require any additional licenses.

Guidelines for ASA FirePOWER

Failover Guidelines

Does not support failover directly; when the ASA fails over, any existing ASA FirePOWER flows are transferred to the new ASA. The ASA FirePOWER module in the new ASA begins inspecting the traffic from that point forward; old inspection states are not transferred.
You are responsible for maintaining consistent policies on the ASA FirePOWER modules in the high-availability ASA pair to ensure consistent failover behavior.

**Note**
Create the failover pair before you configure the ASA FirePOWER modules. If the modules are already configured on both devices, clear the interface configuration on the standby device before creating the high-availability pair. From the CLI on the standby device, enter the `clear configure interface` command.

**ASA Clustering Guidelines**

Does not support clustering directly, but you can use these modules in a cluster. You are responsible for maintaining consistent policies on the ASA FirePOWER modules in the cluster.

**Note**
Create the cluster before you configure the ASA FirePOWER modules. If the modules are already configured on the slave devices, clear the interface configuration on the devices before adding them to the cluster. From the CLI, enter the `clear configure interface` command.

**Model Guidelines**

- For ASA model software and hardware compatibility with the ASA FirePOWER module, see the Cisco ASA Compatibility.
- For the ASA 5515-X through ASA 5555-X, you must install a Cisco solid state drive (SSD). For more information, see the ASA 5500-X hardware guide. (The SSD is standard on the 5508-X, and 5516-X.)
- You cannot change the software type installed on the ASA 5585-X hardware module. If you purchase an ASA FirePOWER module, you cannot later install other software on it.
- The interfaces on the ASA 5585-X ASA FirePOWER hardware module drop traffic for up to 30 seconds during a module reboot, including reboots that occur during a software upgrade.

**ASDM Guidelines for Managing ASA FirePOWER**

- The ASA, ASDM, and ASA FirePOWER versions supported for ASDM management differ by model. For supported combinations, see Cisco ASA Compatibility.
- If you enable command authorization on the ASA that hosts the module, you must log in with a user name that has privilege level 15 to see the ASA FirePOWER home, configuration, and monitoring pages. Read-only or monitor-only access to ASA FirePOWER pages other than the status page is not supported.
- If you are using Java 7 update 51 up to Java 8, you need to configure identity certificates for both the ASA and the ASA FirePOWER module. See Install an Identity Certificate for ASDM.
- You can never use both ASDM and Firepower/FireSIGHT Management Center, you must choose one or the other.

**Additional Guidelines and Limitations**

- See Compatibility with ASA Features, on page 118.
• You cannot configure both normal inline mode and inline tap monitor-only mode at the same time on the ASA. Only one type of service policy rule is allowed. In multiple context mode, you cannot configure inline tap monitor-only mode for some contexts, and regular inline mode for others.

Defaults for ASA FirePOWER

The following table lists the default settings for the ASA FirePOWER module.

Table 8: ASA FirePOWER Default Network Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>System software image: 192.168.45.45/24</td>
</tr>
<tr>
<td></td>
<td>Boot image: 192.168.8.8/24</td>
</tr>
<tr>
<td>Gateway</td>
<td>System software image: none</td>
</tr>
<tr>
<td></td>
<td>Boot image: 192.168.8.1/24</td>
</tr>
<tr>
<td>SSH or session Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>System software image:</td>
</tr>
<tr>
<td></td>
<td>• Release 6.0 and following: Admin123</td>
</tr>
<tr>
<td></td>
<td>• Releases prior to 6.0: Sourcefire</td>
</tr>
<tr>
<td></td>
<td>Boot image: Admin123</td>
</tr>
</tbody>
</table>

Perform Initial ASA FirePOWER Setup

Deploy the ASA FirePOWER module in your network, and then choose your management method.

Deploy the ASA FirePOWER Module in Your Network

See the section for your firewall mode and ASA model to determine how to connect the ASA FirePOWER module management interface to your network.

Routed Mode

ASA 5585-X (Hardware Module) in Routed Mode

The ASA FirePOWER module includes separate management interfaces from the ASA.
All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because the Management 1/x interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA management interface (or you could use a data interface). Other options are possible, depending on how you want to connect your network; for example, you can make the Management 1/0 interface outside facing; or you can route between it and a different ASA interface if you have an inside router.

ASA 5508-X through ASA 5555-X (Software Module) in Routed Mode

These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access. Management traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface to reach the Internet.

If you do not configure a name and IP address in the ASA configuration for Management, then the interface belongs exclusively to the module. In this case, the Management interface is not a regular ASA interface, and you can:

1. Configure the ASA FirePOWER IP address to be on the same network as a regular ASA data interface.
2. Specify the data interface as the ASA FirePOWER gateway.
3. Directly connect the Management interface to the data interface (using a Layer2 switch).

See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface.
For the ASA 5508-X, and 5516-X, the default configuration enables the above network deployment; the only change you need to make is to set the module IP address to be on the same network as the ASA inside interface and to configure the module gateway IP address.

For other models, you must remove the ASA-configured name and IP address for Management 0/0 or 1/1, and then configure the other interfaces as indicated above.

**Note**
You can avoid using an external switch if you have extra interfaces that you can assign to an inside bridge group to configure a “soft switch”. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information.

**Note**
If you want to deploy a separate router on the inside network, then you can route between management and inside. In this case, you can manage both the ASA and ASA FirePOWER module on the Management interface with the appropriate configuration changes, including configuring the ASA name and IP address for the Management interface (on the same network as the ASA FirePOWER module address).

## Transparent Mode

**ASA 5585-X (Hardware Module) in Transparent Mode**

The ASA FirePOWER module includes separate management interfaces from the ASA.

All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because this interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface.
If you do not use an inside router, you can manage the ASA over the inside interface (using the BVI IP address) and not use the Management 0/0 interface:

You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group to configure a “soft switch”. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information.

ASA 5508-X through ASA 5555-X, ISA 3000 (Software Module) in Transparent Mode

These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access.

The following figure shows the recommended network deployment for the ASA 5500-X or ISA 3000 with the ASA FirePOWER module:
If you do not use an inside router, you can manage the ASA over the inside interface (using the BVI IP address) and not use the Management interface for ASA management:

You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group to configure a “soft switch”. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information.

---

**Register the ASA FirePOWER Module with a Management Center**

To register the module with a Firepower/FireSIGHT Management Center, you must access the ASA FirePOWER module CLI. The first time you access the CLI, you are prompted for basic configuration parameters. You must also add the module to the Management Center.

**Notes:**

- If you want to use ASDM to manage the module, skip this section and see Configure the ASA FirePOWER Module for ASDM Management, on page 128.

- If you need to move the module’s management from one management center to another, first remove the device from the management center’s inventory. Then, use the `configure manager add` command to point to the new management center. You can then complete the registration from the new management center. This process ensures a clean hand-over.
Access the ASA FirePOWER CLI

To access the ASA FirePOWER CLI, you can use one of the following methods.

**Procedure**

**Step 1** Console Port:
- ASA 5585-X—This model includes a dedicated console port for the ASA FirePOWER module. Use the supplied DB-9 to RJ-45 serial cable and/or your own USB serial adapter.
- All other models—Connect to the ASA console port using the supplied DB-9 to RJ-45 serial cable and/or your own USB serial adapter. The ASA 5508-X/5516-X also has a mini-USB console port. See the hardware guide for instructions on using the USB console port.

At the ASA CLI, session to the ASA FirePOWER module:

```
session sfr
```

See also Session to the Software Module From the ASA, on page 141.

**Step 2** SSH:
You can connect to the module default IP address (see Defaults for ASA FirePOWER, on page 121) or you can use the following ASA command to change the management IP address, and then connect using SSH:

```
session {1 | sfr} do setup host ip ip_address/mask,gateway_ip
```

Use 1 for a hardware module, sfr for a software module.

**Configure ASA FirePOWER Basic Settings**

The first time you access the ASA FirePOWER module CLI, you are prompted for basic configuration parameters. You must also add the module to the Firepower/FireSIGHT Management Center if you are not using ASDM.

**Before you begin**

Access the module CLI according to Access the ASA FirePOWER CLI, on page 126.

**Procedure**

**Step 1** At the ASA FirePOWER CLI, log in with the username admin.
If this is the first time you are logging in, use the default password. See Defaults for ASA FirePOWER, on page 121.

**Step 2** Complete the system configuration as prompted.

Use the following network settings for the ASA FirePOWER module for the recommended network deployment (Deploy the ASA FirePOWER Module in Your Network, on page 121):

- Management interface: 192.168.1.2
• Management subnet mask: 255.255.255.0
• Gateway IP: 192.168.1.1

Example:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface \{192.168.45.45\}: \{10.86.118.3\}
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' \{\}:
10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' \{example.net\}: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center. A unique alphanumeric registration key is always required. In most cases, to register a sensor to a Defense Center, you must provide the hostname or the IP address along with the registration key.
'configure manager add \{hostname | ip address \} [registration key ]'

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

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

Step 3 Register the ASA FirePOWER module to a Management Center:

> configure manager add \{hostname | IPv4_address | IPv6_address | DONTRESOLVE\} reg_key [nat_id]

where:

• \{hostname | IPv4_address | IPv6_address | DONTRESOLVE\} specifies either the fully qualified hostname or IP address of the Management Center. If the Management Center is not directly addressable, use DONTRESOLVE.

• reg_key is the unique alphanumeric registration key required to register a ASA FirePOWER module to the Management Center.

• nat_id is an optional alphanumeric string used during the registration process between the Management Center and the ASA FirePOWER module. It is required if the hostname is set to DONTRESOLVE.

Step 4 Close the console connection. For the software module, enter:
Configure the ASA FirePOWER Module for ASDM Management

Not supported for all version/model combinations; check for compatibility with your model and version.

ASDM can change the ASA FirePOWER module IP address over the ASA backplane, but all further management requires network access between the ASDM interface and the Management interface, where the module is reachable.

To use ASDM to manage the module, launch ASDM and run the Startup Wizard.

Procedure

Step 1  On the computer connected to the ASA, launch a web browser.
Step 2  In the Address field, enter the following URL: **https://192.168.1.1/admin**. The Cisco ASDM web page appears.
Step 3  Click one of the available options: Install ASDM Launcher, Run ASDM, or Run Startup Wizard.
Step 4  Follow the onscreen instructions to launch ASDM according to the option you chose. The Cisco ASDM-IDM Launcher appears.

**Note**  If you click Install ASDM Launcher, in some cases you need to install an identity certificate for the ASA and a separate certificate for the ASA FirePOWER module according to Install an Identity Certificate for ASDM.

Step 5  Leave the username and password fields empty, and click OK. The main ASDM window appears.
Step 6  If you are prompted to provide the IP address of the installed ASA Firepower module, cancel out of the dialog box. You must first set the module IP address to the correct IP address using the Startup Wizard.
Step 7  Choose Wizards > Startup Wizard.
Step 8  Configure additional ASA settings as desired, or skip screens until you reach the ASA Firepower Basic Configuration screen.
Set the following values to work with the default configuration:

- **IP Address**—192.168.1.2
- **Subnet Mask**—255.255.255.0
- **Gateway**—192.168.1.1

**Step 9**  
Click I accept the agreement, and click **Next** or **Finish** to complete the wizard.

**Step 10**  
Quit ASDM, and then relaunch. You should see **ASA Firepower** tabs on the **Home** page.
Configure the ASA FirePOWER Module

Configure the security policy in the ASA FirePOWER module, and then configure the ASA to send traffic to the module.

Configure the Security Policy on the ASA FirePOWER Module

The security policy controls the services provided by the module, such as Next Generation IPS filtering and application filtering. You configure the security policy on the ASA FirePOWER module using one of the following methods.

**FireSIGHT Management Center**

Use a web browser to open https://DC_address, where DC_address is the DNS name or IP address of the manager you defined in Configure ASA FirePOWER Basic Settings, on page 126. For example, https://dc.example.com.

Alternatively, in ASDM, choose Home > ASA FirePOWER Status and click the link at the bottom of the dashboard.


**ASDM**

In ASDM, choose Configuration > ASA FirePOWER Configuration.


Redirect Traffic to the ASA FirePOWER Module

For inline and inline tap (monitor-only) modes, you configure a service policy to redirect traffic to the module. If you want passive monitor-only mode, you configure a traffic redirection interface, which bypasses ASA policies.

The following topics explain how to configure these modes.

**Configure Inline or Inline Tap Monitor-Only Modes**

Redirect traffic to the ASA FirePOWER module by creating a service policy that identifies specific traffic that you want to send. In this mode, ASA policies, such as access rules, are applied to the traffic before it is redirected to the module.
Before you begin

- If you have an active service policy redirecting traffic to an IPS or CX module (that you replaced with ASA FirePOWER), you must remove that policy before you configure the ASA FirePOWER service policy.
- Be sure to configure consistent policies on the ASA and the ASA FirePOWER module. Both policies should reflect the inline or inline tap mode of the traffic.
- In multiple context mode, perform this procedure within each security context.

Procedure

Step 1
Create an L3/L4 class map to identify the traffic that you want to send to the module.

class-map name
match parameter

Example:

hostname(config)# class-map firepower_class_map
hostname(config-cmap)# match access-list firepower

If you want to send multiple traffic classes to the module, you can create multiple class maps for use in the service policy. For information on matching statements, see Identify Traffic (Layer 3/4 Class Maps), on page 295.

Step 2
Add or edit a policy map that sets the actions to take with the class map traffic: policy-map name

Example:

hostname(config)# policy-map global_policy

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name.

Step 3
Identify the class map you created at the start of this procedure: class name

Example:

hostname(config-pmap)# class firepower_class_map

Step 4
Send the traffic to the ASA FirePOWER module.

sfr {fail-close | fail-open} [monitor-only]

Where:

- The fail-close keyword sets the ASA to block all traffic if the ASA FirePOWER module is unavailable.
- The fail-open keyword sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
• Specify **monitor-only** to send a read-only copy of traffic to the module, i.e. inline tap mode. If you do not include the keyword, the traffic is sent in inline mode. See [ASA FirePOWER Inline Tap Monitor-Only Mode](#), on page 117 for more information.

**Example:**

```bash
hostname(config-pmap-c)# sfr fail-close
```

**Step 5** If you created multiple class maps for ASA FirePOWER traffic, you can specify another class for the policy and apply the `sfr` redirect action.

See [Feature Matching Within a Service Policy](#), on page 287 for detailed information about how the order of classes matters within a policy map. Traffic cannot match more than one class map for the same action type.

**Step 6** If you are editing an existing service policy (such as the default global policy called `global_policy`), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Example:**

```bash
hostname(config)# service-policy global_policy global
```

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

---

### Configure Passive Traffic Forwarding

If you want to operate the module in passive monitor-only mode, where the module gets a copy of the traffic and neither it nor the ASA can affect the network, configure a traffic forwarding interface and connect the interface to a SPAN port on a switch. For more details, see [ASA FirePOWER Passive Monitor-Only Traffic Forwarding Mode](#), on page 117.

The following guidelines explain the requirements for this deployment mode:

- The ASA must be in single-context and transparent mode.
- You can configure up to 4 interfaces as traffic-forwarding interfaces. Other ASA interfaces can be used as normal.
- Traffic-forwarding interfaces must be physical interfaces, not VLANs or BVIs. The physical interface also cannot have any VLANs associated with it.
- Traffic-forwarding interfaces cannot be used for ASA traffic; you cannot name them or configure them for ASA features, including failover or management-only.
- You cannot configure both a traffic-forwarding interface and a service policy for ASA FirePOWER traffic.
**Procedure**

**Step 1** Enter interface configuration mode for the physical interface you want to use for traffic-forwarding.

```
interface physical_interface
```

**Example:**

```
hostname(config)# interface gigabitethernet 0/5
```

**Step 2** Remove any name configured for the interface. If this interface was used in any ASA configuration, that configuration is removed. You cannot configure traffic-forwarding on a named interface.

```
no nameif
```

**Step 3** Enable traffic-forwarding.

```
traffic-forward sfr monitor-only
```

**Note** You can ignore any warnings about traffic forwarding being for demonstration purposes only. This is a supported production mode.

**Step 4** Enable the interface.

```
no shutdown
```

Repeat for any additional interfaces.

**Example**

The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
no nameif
traffic-forward sfr monitor-only
no shutdown
```

**Enable Captive Portal for Active Authentication**

ASA FirePOWER includes identity policies that allow you to collect user identification information. By collecting user identity information, you can tailor access control rules to specific users and user groups, selectively allowing and disallowing access based on the user. You can also analyze traffic based on user identity.

For HTTP/HTTPS connections, you can define identity rules that collect user identification through active authentication. If you want to implement active authentication identity rules, you must enable captive portal on the ASA to act as the authentication proxy port. When a connection matches an identity rule that requests active authentication, the ASA FirePOWER module redirects the authentication request to the ASA interface IP address/captive portal. The default port is 885, which you can change.

If you do not enable captive portal for the authentication proxy, only passive authentication is available.
Before you begin

- This feature is available in routed mode only for ASA FirePOWER 6.0+ only.
- In multiple context mode, perform this procedure within each security context.

Procedure

Step 1
Enable captive portal.

captive-portal {global | interface name} [port number]

Where:

- `global` enables captive portal globally on all interfaces.
- `interface name` enables captive portal on the specified interface only. You can enter the command multiple times to enable it on more than one interface. You can use this approach if you are redirecting traffic for only a subset of interfaces to the ASA FirePOWER module.
- `port number` optionally specifies the authentication port. If you do not include the keyword, port 885 is used. If you do include the keyword, the port number must be 1025 or higher.

Example:

For example, to enable captive portal globally on port 885, enter the following:

```bash
ciscoasa(config)# captive-portal global
```

Step 2
In the ASA FirePOWER identity policy, ensure that the active authentication settings specify the same port you configured for captive portal, and configure the other required settings to enable active authentication.

Managing the ASA FirePOWER Module

This section includes procedures that help you manage the module.

Install or Reimage the Module

This section describes how to install or reimage a software or hardware module.

Install or Reimage the Software Module

If you purchase the ASA with the ASA FirePOWER module, the module software and required solid state drives (SSDs) come pre-installed and ready to configure. If you want to add the ASA FirePOWER software module to an existing ASA, or need to replace the SSD, you need to install the ASA FirePOWER boot software, partition the SSD, and install the system software according to this procedure.

Reimaging the module is the same procedure, except you should first uninstall the ASA FirePOWER module. You would reimage a system if you replace an SSD.
For information on how to physically install the SSD, see the ASA hardware guide.

**Before you begin**

- The free space on flash (disk0) should be at least 3GB plus the size of the boot software.
- In multiple context mode, perform this procedure in the system execution space.
- You must shut down any other software module that you might be running; the ASA can run a single software module at a time. You must do this from the ASA CLI. For example, the following commands shut down and uninstall the IPS software module, and then reload the ASA; the commands to remove the CX module are the same, except use the `cxsc` keyword instead of `ips`.

```
sw-module module ips shutdown
sw-module module ips uninstall
reload
```

When reimaging the ASA FirePOWER module, use the same shutdown and uninstall commands to remove the old image. For example, `sw-module module sfr uninstall`.

- If you have an active service policy redirecting traffic to an IPS or CX module, you must remove that policy. For example, if the policy is a global one, you could use `no service-policy ips_policy global`. If the service policy includes other rules you want to maintain, simply remove the redirection command from the relevant policy map, or the entire traffic class if redirection is the only action for the class. You can remove the policies using CLI or ASDM.
- Obtain both the ASA FirePOWER Boot Image and System Software packages from Cisco.com.

**Procedure**

**Step 1** Download the boot image to the ASA. Do not transfer the system software; it is downloaded later to the SSD. You have the following options:

- ASDM—First, download the boot image to your workstation, or place it on an FTP, TFTP, HTTP, HTTPS, SMB, or SCP server. Then, in ASDM, choose **Tools > File Management**, and then choose the appropriate **File Transfer** command, either **Between Local PC and Flash** or **Between Remote Server and Flash**. Transfer the boot software to disk0 on the ASA.

```
ciscoasa# copy tftp://10.1.1.89/asasfr-5500x-boot-5.4.1-58.img disk0:/asasfr-5500x-boot-5.4.1-58.img
```

- ASA CLI—First, place the boot image on a TFTP, FTP, HTTP, or HTTPS server, then use the `copy` command to download it to flash. The following example uses TFTP.

```
ciscoasa# copy tftp://10.1.1.89/asasfr-5500x-boot-5.4.1-58.img disk0:/asasfr-5500x-boot-5.4.1-58.img
```

**Step 2** Download the ASA FirePOWER system software from Cisco.com to an HTTP, HTTPS, or FTP server accessible from the ASA FirePOWER management interface. Do not download it to disk0 on the ASA.

**Step 3** Set the ASA FirePOWER module boot image location in ASA disk0 by entering the following command:

```
sw-module module sfr recover configure image disk0:file_path
```

**Example:**

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-boot-5.4.1-58.img
```

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10
hostname# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-5.4.1-58.img

If you see a message like “ERROR: Another service (cxsc) is running, only one service is allowed to run at any time,” it means that you already have a different software module configured. You must shut it down and remove it to install a new module as described in the prerequisites section above.

**Step 4**
Load the ASA FirePOWER boot image:

```
sw-module module sfr recover boot
```

**Step 5**
Wait approximately 5-15 minutes for the ASA FirePOWER module to boot up, and then open a console session to the now-running ASA FirePOWER boot image. You might need to press enter after opening the session to get to the login prompt. The default username is **admin** and the default password is **Admin123**.

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123

If the module boot has not completed, the `session` command will fail with a message about not being able to connect over ttyS1. Wait and try again.

**Step 6**
Configure the system so that you can install the system software package:

```
asasfr-boot> setup
```

**Example:**

```
asasfr-boot> setup
Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []
```

You are prompted for the following. Note that the management address and gateway, and DNS information, are the key settings to configure.

- **Host name**—Up to 65 alphanumeric characters, no spaces. Hyphens are allowed.
- **Network address**—You can set static IPv4 or IPv6 addresses, or use DHCP (for IPv4) or IPv6 stateless autoconfiguration.
- **DNS information**—You must identify at least one DNS server, and you can also set the domain name and search domain.
- **NTP information**—You can enable NTP and configure the NTP servers, for setting system time.

**Step 7**
Install the System Software image:

```
asasfr-boot> system install [noconfirm] url
```
Include the `noconfirm` option if you do not want to respond to confirmation messages. Use an HTTP, HTTPS, or FTP URL; if a username and password are required, you will be prompted to supply them.

When installation is complete, the system reboots. The time required for application component installation and for the ASA FirePOWER services to start differs substantially: high-end platforms can take 10 or more minutes, but low-end platforms can take 60-80 minutes or longer. (The `show module sfr` output should show all processes as Up.)

For example:

```bash
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
  Description: Cisco ASA-FirePOWER 5.4.1-58 System Install
  Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.

(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):
The system is going down for reboot NOW!
Console session with module sfr terminated.
```

**Step 8**
Open a session to the ASA FirePOWER module. You will see a different login prompt because you are logging into the fully functional module.

```
ciscoasa# session sfr console
```

**Example:**

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Sourcefire ASA5555 v5.4.1 (build 58)
Sourcefire3D login:
```

**Step 9**
See Configure ASA FirePOWER Basic Settings, on page 126 to complete the setup.

---

**Reimage the 5585-X ASA FirePOWER Hardware Module**

If you need to reimage the ASA FirePOWER hardware module in an ASA 5585-X for any reason, you need to install both the Boot Image and a System Software package, in that order. You must install both packages to have a functioning system. Under normal circumstances, you do not need to reimage the system to install upgrade packages.
To install the boot image, you need to TFTP boot the image from the Management-0 port on the ASA FirePOWER SSP by logging into the module’s Console port. Because the Management-0 port is on an SSP in the first slot, it is also known as Management1/0, but ROMMON recognizes it as Management-0 or Management0/1.

**Note**
The interfaces on the ASA 5585-X ASA FirePOWER hardware module drop traffic for up to 30 seconds during a module reboot, including reboots that occur during a module reimage.

**Before you begin**
To accomplish a TFTP boot, you must:
- Place the Boot Image and a System Software package on a TFTP server that can be accessed through the Management1/0 interface on the ASA FirePOWER module.
- Connect Management1/0 to the network. You must use this interface to TFTP boot the Boot Image.

**Procedure**

**Step 1**
Connect to the module console port.

**Step 2**
Reload the system:

```
  system reboot
```

**Step 3**
When prompted, break out of the boot by pressing Esc. If you see grub start to boot the system, you have waited too long.

This will place you at the ROMMON prompt.

**Step 4**
At the ROMMON prompt, enter:

```
  set
```

Configure the following parameters:
- ADDRESS—The management IP address of the module.
- SERVER—The IP address of the TFTP server.
- GATEWAY—The gateway address to the TFTP server. If the TFTP server is directly attached to Management1/0, use the IP address of the TFTP server. If the TFTP server and management address are on the same subnet, do not configure the gateway or TFTP boot will fail.
- IMAGE—The Boot Image path and image name on the TFTP server. For example, if you place the file on the TFTP server in /tftpboot/images/filename.img, the IMAGE value is images/filename.img.

**Example:**

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfrboot-5.4.1-58.img
```
Step 5  Save the settings:

    sync

Step 6  Initiate the download and boot process:

    tftp

You will see ! marks to indicate progress. When the boot completes after several minutes, you will see a login prompt.

Step 7  Log in as admin, with the password Admin123.

Step 8  Configure the system so that you can install the system software package:

    setup

You are prompted for the following. Note that the management address and gateway, and DNS information, are the key settings to configure.

- Host name—Up to 65 alphanumeric characters, no spaces. Hyphens are allowed.
- Network address—You can set static IPv4 or IPv6 addresses, or use DHCP (for IPv4) or IPv6 stateless autoconfiguration.
- DNS information—You must identify at least one DNS server, and you can also set the domain name and search domain.
- NTP information—You can enable NTP and configure the NTP servers, for setting system time.

Step 9  Install the System Software image:

    system install [noconfirm] url

Example:

    asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg

Include the noconfirm option if you do not want to respond to confirmation messages.

When installation is complete, the system reboots. Allow 10 or more minutes for application component installation and for the ASA FirePOWER services to start.

Step 10 When the boot completes, log in as admin with the default password. See Defaults for ASA FirePOWER, on page 121.

Step 11 See Configure ASA FirePOWER Basic Settings, on page 126 to complete the setup.

---

**Reset the Password**

If you forget the password for the admin user, another user with CLI Configuration permissions can log in and change the password.

If there are no other users with the required permissions, you can reset the admin password from the ASA. The default password differs based on software release; see Defaults for ASA FirePOWER, on page 121.
Before you begin

- In multiple context mode, perform this procedure in the system execution space.
- The password-reset option on the ASA hw-module and sw-module commands does not work with ASA FirePOWER.

Procedure

Reset the module password for the user admin to the default:

```
session {1 | sfr} do password-reset
```

Use 1 for a hardware module, sfr for a software module.

---

Reload or Reset the Module

You can reload, or to reset and then reload, the module from the ASA.

Before you begin

In multiple context mode, perform this procedure in the system execution space.

Procedure

Enter one of the following commands:

- Hardware module (ASA 5585-X):
  
  `hw-module module 1 {reload | reset}
  
  Note: The interfaces on the ASA 5585-X ASA FirePOWER hardware module drop traffic for up to 30 seconds during a module reboot, including reboots that occur during a software upgrade.

- Software module (all other models):
  
  `sw-module module sfr {reload | reset}

---

Shut Down the Module

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

Before you begin

- In multiple context mode, perform this procedure in the system execution space.
• If you reload the ASA, the module is not automatically shut down, so we recommend shutting down the module before reloading the ASA.

Procedure

Enter one of the following commands:

- Hardware module (ASA 5585-X):
  hw-module module 1 shutdown
- Software module (all other models):
  sw-module module sfr shutdown

Uninstall a Software Module Image

You can uninstall a software module image and its associated configuration.

Before you begin
In multiple context mode, perform this procedure in the system execution space.

Procedure

Step 1
Uninstall the software module image and associated configuration.

sw-module module sfr uninstall

Example:

ciscoasa# sw-module module sfr uninstall

Module sfr will be uninstalled. This will completely remove the disk image associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]

Step 2
Reload the ASA.

reload

You must reload the ASA before you can install a new module.

Session to the Software Module From the ASA

Use the ASA FirePOWER CLI to configure basic network settings and to troubleshoot the module.
To access the ASA FirePOWER software module CLI from the ASA, you can session from the ASA. (You cannot session to a hardware module running on a 5585-X.)

You can either session to the module (using Telnet) or create a virtual console session. A console session might be useful if the control plane is down and you cannot establish a Telnet session. In multiple context mode, session from the system execution space.

In either a Telnet or a Console session, you are prompted for a username and password. You can log in with any username configured on the ASA FirePOWER. Initially, the admin username is the only one configured (and it is always available). The initial default password differs based on the type of image (full image or boot image) and software release; see Defaults for ASA FirePOWER, on page 121.

- **Telnet session:**

  session sfr

  When in the ASA FirePOWER CLI, to exit back to the ASA CLI, enter any command that would log you out of the module, such as logout or exit, or press Ctrl-Shift-6, x.

- **Console session:**

  session sfr console

  The only way out of a console session is to press Ctrl-Shift-6, x. Logging out of the module leaves you at the module login prompt.

---

**Note**

Do not use the `session sfr console` command in conjunction with a terminal server where Ctrl-Shift-6, x is the escape sequence to return to the terminal server prompt. Ctrl-Shift-6, x is also the sequence to escape the ASA FirePOWER console and return to the ASA prompt. Therefore, if you try to exit the ASA FirePOWER console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the ASA, the ASA FirePOWER console session is still active; you can never exit to the ASA prompt. You must use a direct serial connection to return the console to the ASA prompt. Use the `session sfr` command instead of the console command when facing this situation.

---

**Upgrade the System Software**

Before applying an upgrade, ensure that the ASA is running the minimum required release for the new version; you might need to upgrade the ASA prior to upgrading the module. For more information about applying upgrades, see the Management Center online help, FireSIGHT System User Guide 5.4, or Firepower Management Center Configuration Guide 6.0.

For ASDM management, you can apply upgrades to the system software and components using Configuration > ASA FirePOWER Configuration > Updates. Click Help on the Updates page for more information.

**Monitoring the ASA FirePOWER Module**

The following topics provide guidance on monitoring the module. For ASA FirePOWER-related syslog messages, see the syslog messages guide. ASA FirePOWER syslog messages start with message number 434001.
Showing Module Status

To check the status of a module, enter one of the following commands:

• **show module [1 | sfr] [details]**

  Shows the status of modules. Include the 1 (for hardware modules) or sfr (for software modules) keyword to see status specific to the ASA FirePOWER module. Include the details keyword to get additional information, including the address of the device that manages the module.

• **show module sfr recover**

  Displays the location of the boot image used when installing the module.

The following is sample output from the `show module` command for an ASA 5585-X with an ASA FirePOWER hardware module installed:

```plaintext
hostname# show module
Mod  Card Type          Model  Serial No.          
----  --------------  ----------  ------------------  
0     ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10  JAF1507AMKE
1     ASA 5585-X FirePOWER Security Services Processor ASA5585-SSP-SFR10  JAF1510BLSA

Mod  MAC Address Range   Hw Version   Fw Version   Sw Version
----  -------------------  -----------  ------------  -----------
0     5475.d05b.1100 to 5475.d05b.110b  1.0        2.0(7)0 100.10(0)8
1     5475.d05b.2450 to 5475.d05b.245b  1.0        2.0(13)0 5.3.1-44

Mod  SSM Application Name  Status  SSM Application Version
----  -------------------  -------  -------------------
1     FirePOWER Up 5.3.1-44

Mod  Status  Data Plane Status  Compatibility
----  ---------  ------------------  ------------
0     Up  Sys  Not Applicable
1     Up  Up

The following example shows the details for a software module. Note that DC Addr indicates the address of the Management Center that manages this device.

hostname# show module sfr details
Getting details from the Service Module, please wait...

Card Type: FirePOWER Services Software Module
Model: ASA5555
Hardware version: N/A
Serial Number: FCH1714J6HP
Firmware version: N/A
Software version: 5.3.1-100
MAC Address Range: bc16.6520.1dcb to bc16.6520.1dcb
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 5.3.1-100
Data Plane Status: Up
Status: Up
DC addr: 10.89.133.202
Mgmt IP addr: 10.86.118.7
Mgmt Network mask: 255.255.252.0
Mgmt Gateway: 10.86.116.1
Mgmt web ports: 443
Mgmt TLS enabled: true

The following example shows the location of the ASA FirePOWER boot image that was used with the `sw-module module sfr recover` command when installing the module.

```
hostname# show module sfr recover
Module sfr recover parameters...
Boot Recovery Image: No
Image File Path: disk0:/asasfr-5500x-boot-5.4.1-58.img
```

**Showing Module Statistics**

Use the `show service-policy sfr` command to display statistics and status for each service policy that includes the `sfr` command. Use `clear service-policy` to clear the counters.

The following example shows the ASA FirePOWER service policy and the current statistics as well as the module status. In monitor-only mode, the input counters remain at zero.

```
ciscoasa# show service-policy sfr
Global policy:
  Service-policy: global_policy
  Class-map: my-sfr-class
    SFR: card status Up, mode fail-close
      packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

**Monitoring Module Connections**

To show connections through the ASA FirePOWER module, enter one of the following commands:

- **show asp table classify domain sfr**
  Shows the NP rules created to send traffic to the ASA FirePOWER module.

- **show asp drop**
  Shows dropped packets. The drop types are explained below.

- **show conn**
  Shows if a connection is being forwarded to a module by displaying the ‘X - inspected by service module’ flag.

The `show asp drop` command can include the following drop reasons related to the ASA FirePOWER module.

**Frame Drops:**

- `sfr-bad-tlv-received`—This occurs when ASA receives a packet from FirePOWER without a Policy ID TLV. This TLV must be present in non-control packets if it does not have the Standby/Active bit set in the actions field.
• sfr-request—The frame was requested to be dropped by FirePOWER due a policy on FirePOWER whereby FirePOWER would set the actions to Deny Source, Deny Destination, or Deny Pkt. If the frame should not have been dropped, review the policies on the module that are denying the flow.

• sfr-fail-close—The packet is dropped because the card is not up and the policy configured was ‘fail-close’ (rather than ‘fail-open’ which allows packets through even if the card was down). Check card status and attempt to restart services or reboot it.

• sfr-fail—The FirePOWER configuration was removed for an existing flow and we are not able to process it through FirePOWER it will be dropped. This should be very unlikely.

• sfr-malformed-packet—The packet from FirePOWER contains an invalid header. For instance, the header length may not be correct.

• sfr-ha-request—This counter is incremented when the security appliance receives a FirePOWER HA request packet, but could not process it and the packet is dropped.

• sfr-invalid-encap—This counter is incremented when the security appliance receives a FirePOWER packet with invalid message header, and the packet is dropped.

• sfr-bad-handle-received—Received Bad flow handle in a packet from FirePOWER Module, thus dropping flow. This counter is incremented, flow and packet are dropped on ASA as the handle for FirePOWER flow has changed in flow duration.

• sfr-rx-monitor-only—This counter is incremented when the security appliance receives a FirePOWER packet when in monitor-only mode, and the packet is dropped.

Flow Drops:
• sfr-request—The FirePOWER requested to terminate the flow. The actions bit 0 is set.
• reset-by-sfr—The FirePOWER requested to terminate and reset the flow. The actions bit 1 is set.
• sfr-fail-close—The flow was terminated because the card is down and the configured policy was 'fail-close'.

Examples for the ASA FirePOWER Module

The following example diverts all HTTP traffic to the ASA FirePOWER module, and blocks all HTTP traffic if the module fails for any reason:

```sh
hostname(config)# access-list ASASFR permit tcp any any eq 80
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list ASASFR
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-close
hostname(config-pmap-c)# service-policy my-sfr-policy global
```

The following example diverts all IP traffic destined for the 10.1.0 network and the 10.2.0 network to the ASA FirePOWER module, and allows all traffic through if the module fails for any reason.

```sh
hostname(config)# access-list my-sfr-acl permit ip any 10.1.0.0 255.255.255.0
hostname(config)# access-list my-sfr-acl2 permit ip any 10.2.0.0 255.255.255.0
hostname(config)# class-map my-sfr-class
```
### History for the ASA FirePOWER Module

<table>
<thead>
<tr>
<th>Feature</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5585-X (all models) support for the matching ASA FirePOWER SSP hardware module. ASA 5512-X through ASA 5555-X support for the ASA FirePOWER software module.</td>
<td>ASA 9.2(2.4) ASA FirePOWER 5.3.1</td>
<td>The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). You can use the module in single or multiple context mode, and in routed or transparent mode. We introduced or modified the following commands: <code>capture interface asa_dataplane</code>, <code>debug sfr</code>, <code>hw-module module 1 reload</code>, <code>hw-module module 1 reset</code>, <code>hw-module module 1 shutdown</code>, <code>session do setup host ip</code>, <code>session do get-config</code>, <code>session do password-reset</code>, <code>session sfr</code>, <code>sfr</code>, <code>show asp table</code>, <code>classify domain sfr</code>, <code>show capture</code>, <code>show conn</code>, <code>show module sfr</code>, <code>show service-policy</code>, <code>sw-module sfr</code>.</td>
</tr>
<tr>
<td>ASA 5506-X support for the ASA FirePOWER software module, including support for configuring the module in ASDM</td>
<td>ASA 9.3(2) ASDM 7.3(3) ASA FirePOWER 5.4.1</td>
<td>You can run the ASA FirePOWER software module on the ASA 5506-X. You can manage the module using FireSIGHT Management Center, or you can use ASDM.</td>
</tr>
<tr>
<td>ASA FirePOWER passive monitor-only mode using traffic redirection interfaces</td>
<td>ASA 9.3(2) ASA FirePOWER 5.4.1</td>
<td>You can now configure a traffic forwarding interface to send traffic to the module instead of using a service policy. In this mode, neither the module nor the ASA affects the traffic. We fully supported the following command: <code>traffic-forward sfr monitor-only</code>. You can configure this in CLI only.</td>
</tr>
<tr>
<td>Support for managing the module through ASDM for the 5506H-X, 5506W-X, 5508-X, and 5516-X.</td>
<td>ASA 9.4(1) ASDM 7.4(1) ASA FirePOWER 5.4.1</td>
<td>You can manage the module using ASDM instead of using FireSIGHT Management Center. No new screens or commands were added.</td>
</tr>
<tr>
<td>Feature</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Support for managing the module through ASDM for the 5512-X through 5585-X.</td>
<td>ASA 9.5.(1.5)</td>
<td>You can manage the module using ASDM instead of using Firepower Management Center (formerly FireSIGHT Management Center).</td>
</tr>
<tr>
<td></td>
<td>ASDM 7.5(1.112)</td>
<td>No new screens or commands were added.</td>
</tr>
<tr>
<td></td>
<td>ASA FirePOWER 6.0</td>
<td></td>
</tr>
<tr>
<td>Captive portal for active authentication on ASA FirePOWER 6.0.</td>
<td>ASA 9.5.(2)</td>
<td>The captive portal feature is required to enable active authentication using identity policies starting with ASA FirePOWER 6.0.</td>
</tr>
<tr>
<td></td>
<td>ASA FirePOWER 6.0</td>
<td>We introduced or modified the following commands:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>captive-portal, clear configure captive-portal, show running-config captive-portal.</td>
</tr>
<tr>
<td>No support in 9.10(1) for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X</td>
<td>9.10(1)</td>
<td>The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1), the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.</td>
</tr>
</tbody>
</table>
Cisco Umbrella

You can configure the device to redirect DNS requests to Cisco Umbrella, so that your FQDN policy defined in Cisco Umbrella can be applied to user connections. The following topics explain how to configure the Umbrella Connector to integrate the device with Cisco Umbrella.

- About Cisco Umbrella Connector, on page 149
- Licensing Requirements for Cisco Umbrella Connector, on page 150
- Guidelines and Limitations for Cisco Umbrella, on page 150
- Configure Cisco Umbrella Connector, on page 152
- Examples for the Umbrella Connector, on page 158
- Monitoring the Umbrella Connector, on page 162
- History for Cisco Umbrella Connector, on page 164

About Cisco Umbrella Connector

If you use Cisco Umbrella, you can configure the Cisco Umbrella Connector to redirect DNS queries to Cisco Umbrella. This allows Cisco Umbrella to identify requests to black- or grey-list domain names and apply your DNS-based security policy.

The Umbrella Connector is part of the system’s DNS inspection. If your existing DNS inspection policy map decides to block or drop a request based on your DNS inspection settings, the request is not forwarded to Cisco Umbrella. Thus, you have two lines of protection: your local DNS inspection policy and your Cisco Umbrella cloud-based policy.

When redirecting DNS lookup requests to Cisco Umbrella, the Umbrella Connector adds an EDNS (Extension mechanisms for DNS) record. An EDNS record includes the device identifier information, organization ID, and client IP address. Your cloud-based policy can use those criteria to control access in addition to the reputation of the FQDN. You can also elect to encrypt the DNS request using DNSCrypt to ensure the privacy of usernames and internal IP addresses.

Cisco Umbrella Enterprise Security Policy

In your cloud-based Cisco Umbrella Enterprise Security policy, you can control access based on the reputation of the fully-qualified domain name (FQDN) in the DNS lookup request. Your Enterprise Security policy can enforce one of the following actions:

- Whitelist—If you have no block rules for an FQDN, and Cisco Umbrella determines that it belongs to a non-malicious site, then the site’s actual IP address is returned. This is normal DNS lookup behavior.
• Greylist—If you have no block rules for an FQDN, and Cisco Umbrella determines that it belongs to a suspicious site, then the DNS reply returns the IP address of the Umbrella intelligent proxy. The proxy can then inspect the HTTP connection and apply URL filtering. You must ensure that intelligent proxy is enabled from the Cisco Umbrella dashboard (Security Setting > Enable Intelligent Proxy).

• Blacklist—If you explicitly block an FQDN, or Cisco Umbrella determines that it belongs to a malicious site, then the DNS reply returns the IP address of the Umbrella cloud landing page for blocked connections.

### Cisco Umbrella Registration

When you configure the Umbrella Connector on a device, it registers with Cisco Umbrella in the cloud. The registration process assigns a single device ID, which identifies one of the following:

- One standalone device in single context mode.
- One high availability pair in single context mode.
- One cluster in single context mode.
- One security context in a multiple-context standalone device.
- One security context of a high availability pair
- One security context of a cluster.

Once registered, the device details will appear on the Cisco Umbrella dashboard. You can then change which policy is attached to a device. During registration, either the policy you specify in the configuration is used, or the default policy is assigned. You can assign the same Umbrella policy to multiple devices. If you specify the policy, the device ID you receive differs from what you would get if you did not specify a policy.

### Licensing Requirements for Cisco Umbrella Connector

To use the Cisco Umbrella Connector, you must have a 3DES license. If you are using Smart Licensing, your account must be enabled for export-controlled functionality.

The Cisco Umbrella portal has separate licensing requirements.

### Guidelines and Limitations for Cisco Umbrella

**Context Mode**

- In multiple-context mode, you configure the Umbrella Connector in each context. Each context has a separate device ID, and is represented as a separate device in the Cisco Umbrella Connector dashboard. The device name is the hostname configured in the context, plus the hardware model, plus the context name. For example, CiscoASA-ASA5515-Context1.

**Failover**

- The active unit in the high availability pair registers the pair as a single unit with Cisco Umbrella. Both peers use the same device ID, which is formed from their serial numbers:
primary_serial_number_secondary_serial_number. For multiple context mode, each pair of security contexts is considered a single unit. You must configure high availability, and the units must have successfully formed a high-availability group (even if the standby device is currently in a failed state), before enabling Cisco Umbrella, or the registration will fail.

Cluster

• The cluster master registers the cluster as a single unit with Cisco Umbrella. All peers use the same device ID. For multiple context mode, a security context in the cluster is considered a single unit across all peers.

Additional Guidelines

• Redirection to Cisco Umbrella is done for DNS requests in through traffic only. DNS requests that the system itself initiates are never redirected to Cisco Umbrella. For example, FQDN-based access control rules are never resolved based on Umbrella policy, nor are any FQDNs that are used in other commands or configuration settings.

• The Cisco Umbrella Connector works on any DNS request in through traffic. However, the blacklist and greylist actions are effective only if the DNS response is then used for HTTP/HTTPS connections, because the IP address returned is for a website. Any blacklisted or greylisted addresses for non-HTTP/HTTPS connections will either fail or complete in a misleading fashion. For example, pinging a blacklisted FQDN would result in pinging the server that hosts the Cisco Umbrella cloud block page.

Note Cisco Umbrella does try to intelligently identify FQDNs that might be non-HTTP/HTTPS, and does not return the IP address to the intelligent proxy for those FQDNs for greylisted domain names.

• The system sends DNS/UDP traffic only to Cisco Umbrella. If you enable DNS/TCP inspection, the system does not send any DNS/TCP requests to Cisco Umbrella. However, DNS/TCP requests do not increment the Umbrella bypass counter.

• If you enable DNScrypt for Umbrella inspection, the system uses UDP/443 for the encrypted session. You must include UDP/443 along with UDP/53 in the class map that applies DNS inspection for Cisco Umbrella for DNScrypt to work correctly. Both UDP/443 and UDP/53 are included in the default inspection class for DNS, but if you create a custom class, ensure that you define an ACL that includes both ports for the match class.

• DNScrypt uses IPv4 only for the certificate update handshake. However, DNScrypt does encrypt both IPv4 and IPv6 traffic.

• Cisco Umbrella and ASA FirePOWER processing are not compatible for a given connection. If you want to use both services, you must exclude UDP/53 and UDP/443 from ASA FirePOWER processing. For example, if you are currently redirecting all traffic to the ASA FirePOWER module, you must update the class to use an access list match. The access list should start by denying any connections to the Umbrella servers on destination ports UDP/53 and UDP/443, then permit any source to any destination. The ACL and match statements would be similar to the following:

access-list sfr extended deny udp any host 208.67.220.220 eq domain
access-list sfr extended deny udp any host 208.67.220.220 eq 443
access-list sfr extended permit ip any any
Configure Cisco Umbrella Connector

You can configure the device to interact with Cisco Umbrella in the cloud. The system redirects DNS lookup requests to Cisco Umbrella, which then applies your cloud-based Enterprise Security fully-qualified domain name (FQDN) policy. For malicious or suspicious traffic, users can be blocked from a site, or redirected to an intelligent proxy that can perform URL filtering based on your cloud-based policy.

The following procedure explains the end-to-end process for configuring the Cisco Umbrella Connector.

**Before you begin**

In multiple-context mode, perform this procedure in each security context that should use Cisco Umbrella.

**Procedure**

**Step 1**

**Step 2**
Install the CA Certificate from the Cisco Umbrella Registration Server, on page 153.

The device registration uses HTTPS, which requires that you install the root certificate.
Install the CA Certificate from the Cisco Umbrella Registration Server

You must import the root certificate to establish the HTTPS connection with the Cisco Umbrella registration server. The system uses the HTTPS connection when registering the device.

Following is the PEM certificate that you must import.

-----BEGIN CERTIFICATE-----
MIIEIIC3ylAwIBAQQIAYIQA2j627KdciniQ4tyS8+8kTANBgkqkhIGil9w0BAGA4FADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgMRkwFwYDVQQEFUKZEd3dvY9
d3cuZGlnaUNlcnQuY29tMA0GCSqGSIb3DQEB
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgMRkwFwYDVQQEFUKZEd3dvY9
d3cuZGlnaUNlcnQuY29tMA0GCSqGSIb3DQEB
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgMRkwFwYDVQQEFUKZEd3dvY9
d3cuZGlnaUNlcnQuY29tMA0GCSqGSIb3DQEB
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgMRkwFwYDVQQEFUKZEd3dvY9
-----END CERTIFICATE-----
Procedure

**Step 1**
Create a trustpoint for the Cisco Umbrella registration server.

```
crypto ca trustpoint name
```
You can use any name you want for the trustpoint (up to 128 characters), such as ctx1 or umbrella_server.

**Example:**
```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

**Step 2**
Indicate that you want to manually enroll by pasting the certificate.

```
enrollment terminal
```

**Example:**
```
ciscoasa(config-ca-trustpoint)# enrollment terminal
```

**Step 3**
Import the certificate.

```
crypto ca authenticate name
```
Enter the name of the trustpoint you created for this certificate. Follow the prompts and paste the base-64 encoded certificate. Do not include the BEGIN CERTIFICATE and END CERTIFICATE lines.

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
MIIElDCCA3ygAwIBAgIQAf2j627Kdc1Oi4ty9S+8kTAHBqkhig19w0BAQesFADBhMQcwQYDVQQEEwJvJ1JzZVEaMBGA1UEcwwMMG1naUN1cnQwS5jMSRkwFwYuQDQTEwB3d3cu2GlnaWN1cnQy929tMSAwh6YDVQQDEwEaWdpQ2VydCBhbmNzaW9uZWNhdGFsb2Jhcy53Oy0x0gU2YdXJK1FN1cnZ1c2BDDCQIwDQYJKoZIhvcnaQEBBQADgEBAQgEAMC5G
```

**CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10**

Install the CA Certificate from the Cisco Umbrella Registration Server
INFO: Certificate has the following attributes:
Fingerprint: 345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)#

---

**Configure the Umbrella Connector Global Settings**

The Umbrella global settings primarily define the API token that is needed to register the device with Cisco Umbrella. The global settings are not sufficient to enable Umbrella. You must also enable Umbrella in your DNS inspection policy map, as described in *Enable Umbrella in the DNS Inspection Policy Map*, on page 156.

**Before you begin**

- Log into the Cisco Umbrella Network Devices Dashboard (https://login.umbrella.com/) and obtain a network device API token for your organization. A token will be a hexadecimal string, for example, AABBA59A0BDE1485C912AFE. In Umbrella, you can find this by selecting **Deployments > Core Identities > Network Devices**. Click the **API Token** button in the upper right of the page if an API token is not already displayed on the page.

- Install the certificate for the Cisco Umbrella registration server.

**Procedure**

**Step 1**
Enter Umbrella configuration mode.

```
umbrella-global
```

**Example:**

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

**Step 2**
Configure the API token needed to register with Cisco Umbrella.

```
token  api_token
```

**Example:**

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
ciscoasa(config-umbrella)#
```

Please make sure all the Umbrella Connector prerequisites are satisfied:

1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
Step 3  
(Optional.) If you intend to enable DNScrypt in the DNS inspection policy map, you can optionally configure the DNScrypt provider public key for certificate verification. If you do not configure the key, the default currently distributed public key is used for validation.

**public-key**  
*hex_key*

The key is a 32-byte hexadecimal value. Enter the hex value in ASCII with a colon separator for every 2 bytes. The key is 79 bytes long. Obtain this key from Cisco Umbrella.

The default key is:

To revert to using the default public key, enter **no public-key**. You can either omit the key you configured, or include it on the **no** version of the command.

**Example:**
```
ciscoasa(config-umbrella)# public-key
```

Step 4  
(Optional.) Configure the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.

**timeout edns hh:mm:ss**

The timeout is in hours:minutes:seconds format, and can be from 0:0:0 to 1193:0:0. The default is 0:02:00 (2 minutes).

**Example:**
```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

---

### Enable Umbrella in the DNS Inspection Policy Map

Configuring the global Umbrella settings is not enough to register the device and enable DNS lookup redirection. You must add Umbrella as part of your active DNS inspection.

You can enable Umbrella globally by adding it to the preset_dns_map DNS inspection policy map.

However, if you have customized DNS inspection and applied different inspection policy maps to different traffic classes, you must enable Umbrella on each class where you want the service.

The following procedure explains how to implement Umbrella globally. If you have customized DNS policy maps, please see Configure DNS Inspection Policy Map, on page 333.

#### Procedure

**Step 1**  
Edit the preset_dns_map inspection policy map and enter parameter configuration mode.
Step 2  Enable Umbrella and optionally specify the name of the Cisco Umbrella policy to apply to the device.

`umbrella [tag umbrella_policy]`

The tag is the name of a policy as defined in Cisco Umbrella. During registration, Cisco Umbrella will assign the policy to the device (if the policy name exists). If you do not specify a policy, the default policy is applied.

Example:

```
ciscoasa(config-pmap-p)# umbrella
```

Step 3  (Optional.) Enable DNScrypt to encrypt connections between the device and Cisco Umbrella.

`dnscrypt`

Enabling DNScrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key. Because DNScrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.

Example:

```
ciscoasa(config-pmap-p)# dnscrypt
```

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

Verify the Umbrella Registration

After you configure the global Umbrella settings and enable Umbrella in DNS inspection, the device should contact Cisco Umbrella and register. You can check for successful registration by checking whether Cisco Umbrella provided a device ID.

First, check the service policy statistics, and look for the Umbrella Registration line. This should indicate the policy applied by Cisco Umbrella (the tag), the HTTP status of the connection (401 indicates that the API token was incorrect, and 409 indicates that the device already exists in Cisco Umbrella), and the device ID.

```
asa(config)# show service-policy inspect dns
Interface inside:
   Service-policy: global_policy
   Class-map: inspection_default
```
Examples for the Umbrella Connector

The following topics provide examples of configuring the Umbrella Connector.

Example: Enabling Umbrella on the Global DNS Inspection Policy

The following example shows how to enable Umbrella globally. The configuration enables DNSCrypt using the default public key. It assigns the default Cisco Umbrella Enterprise Security policy.

ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1

Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself.

```
MIIEiDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuGI1naWNlc3MuY29tMCwwGQYDVQQHEw9EaWdpQ2VydCBJbmNlcyBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCg
```

The following example edits the output to show the relevant information.

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
    umbrella device-id 010a3e5760fdd6d3
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
```

You can also verify the running configuration (filter on policy-map). The umbrella command in the policy map updates to show the device ID. You cannot directly configure the device ID when you enable this command. The following example edits the output to show the relevant information.

```
ciscoasa(config)#
show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
    umbrella device-id 010a3e5760fdd6d3
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
```
INFO: Certificate has the following attributes:
Fingerprint: 345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

% Certificate successfully imported

Example: Enabling Umbrella on an Interface with a Custom Inspection Policy

The following example shows how to enable Umbrella for a specific traffic class. Umbrella is enabled on the inside interface only for DNS/UDP traffic. Because we are enabling DNScrypt, UDP/443 must be included in the traffic class. An Enterprise Security policy named mypolicy (defined in Cisco Umbrella) is applied.

ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

Example: Enabling Umbrella on an Interface with a Custom Inspection Policy
Example: Enabling Umbrella on an Interface with a Custom Inspection Policy

QTAsMoWzAxAygMDn7jAwMgDzAwW0yMzAzMDqzMjAwMDBmbmF0dGhpbmRpbmcA==
MQ0wEwYDVQQKEwxEaWdpQ2VydCBJbmNzdWx0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzhxtniMB8GA1UdIwQyMBaAFAPeUDVW0Uy7Zc4jhsbw5eyPdFMoAGHsQGSIb3DQEBCwAAAAIBAQJq9L0jfcpbzG1wamhpG01X0VvgBCFSs+JtluHdC9l4unMwnQp1q3TjPh0i6bDrOi6b7n45puh72FPLhLqTUq/sElLeFmzqPlt/yGjFUZ2gHb0IDjcl1GA
BMWw5dRmJzSszm8c+cftI17gzb6tOCw6twOuYFfzCETe67S/a/3H480/11LAt7DdC2iDJe6mK7Qq2iWLI1GBtLFry8E7/j8s8e9fX7t8N0Cp1Tm6gcr6UNb0wBhf7U///7TLm46e3o4nJy40Gw5M4C/9A3673BmB0Jh37/72P07kzQ3oH3jO10HvDjPbRzeXDLz

INFO: Certificate has the following attributes:
Fingerprint: 345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported

ciscoasa(config)#
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.222.220
ciscoasa(config)#

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config)# service-object udp destination eq domain
ciscoasa(config)# service-object udp destination eq 443

ciscoasa(config)# service-policy umbrella-acl extended permit

ciscoasa(config)# service-policy inside-policy

ciscoasa(config)# service-policy inside-policy interface inside

ciscoasa(config)#

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10
Cisco Umbrella and ASA FirePOWER processing are not compatible for a given connection. If you want to use both services, you must exclude UDP/53 and UDP/443 from ASA FirePOWER processing. For example, if you are currently redirecting all traffic to the ASA FirePOWER module, you must update the class to use an access list match. The access list should start by denying any connections to the Umbrella servers on destination ports UDP/53 and UDP/443, then permit any source to any destination.

The following example enables both Umbrella and ASA FirePOWER globally. The Umbrella configuration is added to the default DNS inspection map, which is already applied in the global policy.

```cisco
# Enable both Umbrella and ASA FirePOWER
crypto ca trustpoint ctx1

ciscoasa(config)# dns domain-lookup outside

ciscoasa(config)# token AABBA59A0BDE1485C912AFE
```

INFO: Certificate has the following attributes:
Fingerprint: 345eff15 b7a49add 451b65a7 f4bdc6ae
Do you accept this certificate? [yes/no]: yes

Trustpoint 'ctx1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully accepted.
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
  ciscoasa(config-pmap-p)# umbrella
  ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# access-list sfr extended deny udp any host 208.67.220.220 eq domain

ciscoasa(config)# access-list sfr extended deny udp any host 208.67.220.220 eq 443

  ciscoasa(config)# access-list sfr extended permit ip any any

ciscoasa(config)# class-map sfr
    ciscoasa(config-cmap)# match access-list sfr

  ciscoasa(config)# policy-map global_policy
    ciscoasa(config-pmap)# class sfr
    ciscoasa(config-pmap-c)# sfr fail-open

  ciscoasa(config)# service-policy global_policy global
```

## Monitoring the Umbrella Connector

The following topics explain how to monitor the Umbrella Connector.

### Monitoring the Umbrella Service Policy Statistics

You can view both summarized and detailed statistics for DNS inspection with Umbrella enabled.

```
  show service-policy inspect dns [detail]
```

Without the `detail` keyword, you see all the basic DNS inspection counters plus Umbrella configuration information. The status field provides the HTTP status code for the system’s attempt to register with Cisco Umbrella.

```
asa(config)# show service-policy inspect dns
  Interface inside:
    Service-policy: global_policy
      Class-map: inspection_default
        Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
      umbrella registration: tag: default, status: 200 success, device-id: 010a13b8fbdfc9aa

    Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
    DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
    DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
    DNScrypt: Certificate Update: completion 10, failure 1
```
The detailed output shows DNSCrypt statistics and the keys used.

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
  Class-map: dnsCrypt30000
    Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
      5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    message-length maximum client auto, drop 0
    message-length maximum 1500, drop 0
    dns-guard, count 3
    protocol-enforcement, drop 0
    nat-rewrite, count 0
  Umbrella registration: tag: default, status: 200 SUCCESS, device-id: 010af97abf89abc3,
    retry 0
    Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6
      Umbrella app-id fail, count 0
      Umbrella flow alloc fail, count 0
      Umbrella block alloc fail, count 0
      Umbrella client flow expired, count 0
      Umbrella server flow expired, count 0
      Umbrella request drop, count 0
      Umbrella response drop, count 0
  DNSCrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
  DNSCrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
    DNSCrypt length error, count 0
    DNSCrypt add padding error, count 0
    DNSCrypt encryption error, count 0
    DNSCrypt magic_mismatch error, count 0
    DNSCrypt disabled, count 0
    DNSCrypt flow error, count 0
    DNSCrypt nonce error, count 0
  DNSCrypt: Certificate Update: completion 1, failure 1
    DNSCrypt Receive internal drop count 0
    DNSCrypt Receive on wrong channel drop count 0
    DNSCrypt Receive cannot queue drop count 0
    DNSCrypt No memory to create channel count 0
    DNSCrypt Send no output interface count 1
    DNSCrypt Send open channel failed count 0
    DNSCrypt Send no handle count 0
    DNSCrypt Send dupb failure count 0
    DNSCrypt Create cert update no memory count 0
    DNSCrypt Store cert no memory count 0
    DNSCrypt Certificate invalid length count 0
    DNSCrypt Certificate invalid magic count 0
    DNSCrypt Certificate invalid major version count 0
    DNSCrypt Certificate invalid minor version count 0
    DNSCrypt Certificate invalid signature count 0
  Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
  Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
  Query Magic 0x714e7a696d657555, Serial Number 1517943461,
  Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
  End Time 1549479461 (18:57:41 UTC Feb 6 2019)
  Server Public Key
Client Secret Key Hash
Client Public key
NM Key Hash
```
Monitoring Umbrella Syslog Messages

You can monitor the following Umbrella-related syslog messages:

- %ASA-3-339001: DNSCRYPT certificate update failed for number tries.
  
  Check that there is a route to the Umbrella server and that the egress interface is up and functioning correctly. Also check that the public key configured for DNScrypt is correct. You might need to obtain a new key from Cisco Umbrella.

- %ASA-3-339002: Umbrella device registration failed with error code error_code.
  
  The error codes have the following meanings:
  
  - 400—There is a problem with the request format or content. The token is probably too short or corrupted. Verify that the token matches the one on the Umbrella Dashboard.
  
  - 401—The API token is not authorized. Try reconfiguring the token. If you refreshed the token on the Umbrella Dashboard, then you must ensure that you use the new token.
  
  - 409—The device ID conflicts with another organization. Please check with the Umbrella Administrator to see what the issue might be.
  
  - 500—There is an internal server error. Check with the Umbrella Administrator to see what the issue might be.

- %ASA-6-339003: Umbrella device registration was successful.

- %ASA-3-339004: Umbrella device registration failed due to missing token.
  
  You must obtain an API token from Cisco Umbrella and configure it in the global Umbrella settings.

- %ASA-3-339005: Umbrella device registration failed after number retries.
  
  Check the syslog 339002 messages to identify the errors that you need to fix.

History for Cisco Umbrella Connector

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Umbrella support.</td>
<td>9.10(1)</td>
<td>You can configure the device to redirect DNS requests to Cisco Umbrella, so that your Enterprise Security policy defined in Cisco Umbrella can be applied to user connections. You can allow or block connections based on FQDN, or for suspicious FQDNs, you can redirect the user to the Cisco Umbrella intelligent proxy, which can perform URL filtering. The Umbrella configuration is part of the DNS inspection policy. We added or modified the following commands: umbrella, umbrella-global, token, public-key, timeout edns, dnsencrypt, show service-policy inspect dns detail.</td>
</tr>
</tbody>
</table>
Information About Cisco Cloud Web Security

When you enable Cloud Web Security on the ASA, the ASA transparently redirects selected HTTP and HTTPS traffic to the Cloud Web Security proxy servers based on service policy rules. The Cloud Web Security proxy servers then scan the content and allow, block, or send a warning about the traffic based on the policy configured in Cisco ScanCenter to enforce acceptable use and to protect users from malware.

The ASA can optionally authenticate and identify users with Identity Firewall and AAA rules. The ASA encrypts and includes the user credentials (including usernames and user groups) in the traffic it redirects to Cloud Web Security. The Cloud Web Security service then uses the user credentials to match the traffic to the policy. It also uses these credentials for user-based reporting. Without user authentication, the ASA can supply an (optional) default username and group, although usernames and groups are not required for the Cloud Web Security service to apply policy.

You can customize the traffic you want to send to Cloud Web Security when you create your service policy rules. You can also configure a “whitelist” so that a subset of web traffic that matches the service policy rule instead goes directly to the originally requested web server and is not scanned by Cloud Web Security.

You can configure a primary and a backup Cloud Web Security proxy server, each of which the ASA polls regularly to check for availability.
User Identity and Cloud Web Security

You can use user identity to apply policy in Cloud Web Security. User identity is also useful for Cloud Web Security reporting. User identity is not required to use Cloud Web Security. There are other methods to identify traffic for Cloud Web Security policy.

You can use the following methods of determining the identity of a user or of providing a default identity:

- **Identity firewall**—When the ASA uses identity firewall with Active Directory (AD), the username and group is retrieved from the AD agent. Users and groups are retrieved when you use them in an ACL in a feature such as an access rule or in your service policy, or by configuring the user identity monitor to download user identity information directly.

- **AAA rules**—When the ASA performs user authentication using a AAA rule, the username is retrieved from the AAA server or local database. Identity from AAA rules does not include group information. If you configure a default group, these users are associated with that default group. For information about configuring AAA rules, see the legacy feature guide.

- **Default username and group**—For traffic that does not have an associated user name or group, you can configure an optional default username and group name. These defaults are applied to all users that match a service policy rule for Cloud Web Security.

Authentication Keys

Each ASA must use an authentication key that you obtain from Cloud Web Security. The authentication key lets Cloud Web Security identify the company associated with web requests and ensures that the ASA is associated with a valid customer.

You can use one of two types of authentication keys for your ASA: the company key or the group key.

- **Company authentication key**—You can use a company authentication key on multiple ASAs within the same company. This key simply enables the Cloud Web Security service for your ASAs.

- **Group authentication key**—A Group authentication key is a special key unique to each ASA that performs two functions:
  - Enables the Cloud Web Security service for one ASA.
  - Identifies all traffic from the ASA so you can create ScanCenter policy per ASA.

You generate these keys in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp). For more information, see the Cloud Web Security documentation:


ScanCenter Policy

In ScanCenter, traffic is matched against policy rules in order until a rule is matched. Cloud Web Security then applies the configured action for the rule, allowing or blocking the traffic, or warning the user. With warnings, the user has the option to continue on to the web site.

You configure the URL filtering policies in ScanCenter, not in the ASA.
However, part of the policy is to whom the policy applies. User traffic can match a policy rule in ScanCenter based on group association: a directory group or a custom group. Group information is included in the requests redirected from the ASA, so you need to understand what group information you might get from the ASA.

**Directory Groups**

Directory groups define the group to which traffic belongs. When using the identity firewall, the group, if present, is included in the client’s HTTP request. If you do not use identity firewall, you can configure a default group for traffic matching an ASA rule for Cloud Web Security inspection.

In ScanCenter, when you configure a directory group in a policy, you must enter the group name exactly.

- Identity firewall group names are sent in the following format.
  
  \texttt{domain-name\group-name}

  Note that on the ASA, the format is \texttt{domain-name\group-name}. However, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation when including the group in the redirected HTTP request.

- The default group name is sent in the following format:
  
  \texttt{[domain]group-name}

  On the ASA, you need to configure the optional domain name to be followed by 2 backslashes (\\); however, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation. For example, if you specify “Cisco\Boulder1,” the ASA modifies the group name to be “Cisco\Boulder1” with only one backslash (\) when sending the group name to Cloud Web Security.

**Custom Groups**

Custom groups are defined using one or more of the following criteria:

- ScanCenter Group authentication key—You can generate a Group authentication key for a custom group. Then, if you identify this group key when you configure the ASA, all traffic from the ASA is tagged with the Group key.

- Source IP address—You can identify source IP addresses in the custom group. Note that the ASA service policy is based on source IP address, so you might want to configure any IP address-based policy on the ASA instead.

- Username—You can identify usernames in the custom group.

  - Identity firewall usernames are sent in the following format:
    
    \texttt{domain-name\username}

  - AAA usernames, when using RADIUS or TACACS+, are sent in the following format:
    
    \texttt{LOCAL\username}

  - AAA usernames, when using LDAP, are sent in the following format:
    
    \texttt{domain-name\username}

  - For the default username, it is sent in the following format:
    
    \texttt{[domain-name]\username}
How Groups and the Authentication Key Interoperate

Unless you need the per-ASA policy that a custom group plus group key provides, you will likely use a company key. Note that not all custom groups are associated with a group key. You can use non-keyed custom groups to identify IP addresses or usernames, and use them in your policy along with rules that use directory groups.

Even if you do want per-ASA policy and are using a group key, you can also use the matching capability provided by directory groups and non-keyed custom groups. In this case, you might want an ASA-based policy, with some exceptions based on group membership, IP address, or username. For example, if you want to exempt users in the America\Management group across all ASAs:

1. Add a directory group for America\Management.
2. Add an exempt rule for this group.
3. Add rules for each custom group plus group key after the exempt rule to apply policy per-ASA.
4. Traffic from users in America\Management will match the exempt rule, while all other traffic will match the rule for the ASA from which it originated.

Many combinations of keys, groups, and policy rules are possible.

Failover from Primary to Backup Proxy Server

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 minutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active. The ASA determines availability based on the server's ability to complete the TCP three-way handshake.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

You can further refine failover by checking the health of the Cloud Web Security application. In some cases, the server can complete the TCP three-way handshake, yet the Cloud Web Security application on the server is not functioning correctly. If you enable application health checking, the system can fail over to the backup server even if the three-way handshake completes, if the application itself does not respond. This provides a more reliable failover setup.

Health checking involves sending a GET request with a test URL to the Cloud Web Security application. Failure to respond within the configured timeout and retry limits marks the server as down, and the system initiates failover. The backup server is also tested to ensure that it is functioning correctly before it is marked as the active server. After failover, the application on the primary server is retested every 30 seconds until it comes back online and can be marked the active server again.

You can choose how the ASA handles web traffic when it cannot reach either the primary or backup Cloud Web Security proxy server. It can block or allow all web traffic. By default, it blocks web traffic.
Licensing Requirements for Cisco Cloud Web Security

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv</td>
<td>Standard or Premium License.</td>
</tr>
<tr>
<td>All other models</td>
<td>Strong Encryption (3DES/AES) License to encrypt traffic between the ASA and the Cloud Web Security server.</td>
</tr>
</tbody>
</table>

On the Cloud Web Security side, you must purchase a Cisco Cloud Web Security license and identify the number of users that the ASA handles. Then log into ScanCenter and generate your authentication keys.

Guidelines for Cloud Web Security

Failover Guidelines

Supported in failover configurations. However, in Active/Active failover, configure policies on the primary unit only. The Cloud Web Security Connector tracks tower reachability from the primary unit only; the secondary unit will always report the tower as unreachable. Upon failover, when the secondary unit becomes primary, the secondary unit can track tower reachability.

Context Mode Guidelines

Supported in single and multiple context modes.

In multiple context mode, the server configuration is allowed only in the system context, and the service policy rule configuration is allowed only in the security contexts. The Cloud Web Security Connector tracks tower reachability from the primary admin context only.

Each context can have its own authentication key, if desired.

Firewall Mode Guidelines

Supported in routed firewall mode only. Does not support transparent firewall mode.

IPv6 Guidelines

Does not support IPv6. Cloud Web Security currently supports only IPv4 addresses. If you use IPv6 internally, use NAT 64 to translate IPv6 addresses to IPv4 for any IPv6 flows that need to be sent to Cloud Web Security.

Additional Guidelines

- Cloud Web Security is not supported with ASA clustering.
- You cannot use Cloud Web Security on the same traffic you redirect to a module that can also perform URL filtering, such as ASA CX and ASA FirePOWER. The traffic is sent to the modules only, not to the Cloud Web Security servers.
- Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security.
• When an interface to the Cloud Web Security proxy servers goes down, output from the `show scansafe server` command shows both servers up for approximately 15-25 minutes. This condition may occur because the polling mechanism is based on the active connection, and because that interface is down, it shows zero connection, and it takes the longest poll time approach.

• Cloud Web Security inspection is compatible with HTTP inspection for the same traffic.

• Cloud Web Security is not supported with extended PAT or any application that can potentially use the same source port and IP address for separate connections. For example, if two different connections (targeted to separate servers) use extended PAT, the ASA might reuse the same source IP and source port for both connection translations because they are differentiated by the separate destinations. When the ASA redirects these connections to the Cloud Web Security server, it replaces the destination with the Cloud Web Security server IP address and port (8080 by default). As a result, both connections now appear to belong to the same flow (same source IP/port and destination IP/port), and return traffic cannot be untranslated properly.

• The default inspection traffic class does not include the default ports for the Cloud Web Security inspection (80 and 443).

## Configure Cisco Cloud Web Security


Use the following process to configure the ASA to redirect web traffic to Cloud Web Security.

### Before you begin

If you want to send user identity information to Cloud Web Security, configure one of the following on the ASA:

• Identity firewall (username and group).

• AAA rules (username only)—See the legacy feature guide.

If you want to use fully-qualified domain names (FQDN), such as www.example.com, you must configure a DNS server for the ASA.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Communications with the Cloud Web Security Proxy Server, on page 171.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional.) Identify Whitelisted Traffic, on page 173.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure a Service Policy to Send Traffic to Cloud Web Security, on page 175.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional.) Configure the User Identity Monitor, on page 179</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the Cloud Web Security Policy, on page 179.</td>
</tr>
</tbody>
</table>
Configure Communications with the Cloud Web Security Proxy Server

You must identify the Cloud Web Security proxy servers so that user web requests can be redirected properly. In multiple context mode, you must configure the proxy servers in the system context, then enable Cloud Web Security per context. Thus, you can use the service in some contexts but not in others.

Before you begin

- You must configure a DNS server for the ASA to use fully-qualified domain names for the proxy servers.
- (Multiple context mode.) You must configure a route pointing to the Cloud Web Security proxy servers in both the system context and the specific contexts. This ensures that the Cloud Web Security proxy servers do not become unreachable in the Active/Active failover scenario.

Procedure

Step 1 Enter ScanSafe general-options configuration mode. In multiple context mode, do this in the system context.

```
scansafe general-options
```

Example:

```
hostname(config)# scansafe general-options
```

Step 2 Configure the primary and secondary Cloud Web Security proxy servers.

```
server primary {ip ip_address | fqdn fqdn} [port port]
server backup {ip ip_address | fqdn fqdn} [port port]
```

When you subscribe to the Cisco Cloud Web Security service, you are assigned primary and backup Cloud Web Security proxy servers. Enter their IP addresses (ip), or fully-qualified domain names (fqdn), on these commands.

By default, the Cloud Web Security proxy server uses port 8080 for both HTTP and HTTPS traffic; do not change this value unless directed to do so.

Example:

```
hostname(cfg-scansafe)# server primary ip 192.168.43.10
hostname(cfg-scansafe)# server backup fqdn server.example.com
```

Step 3 (Optional.) Configure the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable.

```
retry-count value
```

Polls are performed every 30 seconds. Valid values are from 2 to 100, and the default is 5.

Example:

```
hostname(cfg-scansafe)# retry-count 2
```
Step 4  
(Optional.) Enable application health checking to improve failover processing.
You can configure Cisco Cloud Web Security to check the health of the Cloud Web Security application when determining if the server is healthy. By checking application health, the system can fail over to the backup server when the primary server responds to the TCP three-way handshake but cannot process requests. This ensures a more reliable system.

a) Enable application health checking.

```bash
health-check application [url url_string]
```

Specify a URL only if instructed to do so by Cisco Cloud Web Security. The URL is used when polling the system to determine if the application can respond. The default URL is http://gs.scansafe.net/goldStandard?type=text&size=10. If that URL is no longer the one required, specify the new one given to you by Cisco.

**Example:**

```bash
hostname(cfg-scansafe)# health-check application
```

b) Set the health check polling timeout.

```bash
health-check application timeout seconds
```

The timeout determines how long the ASA waits after sending a GET request for the health check URL to get a response. The ASA retries the request after the timeout up to the retry limit for polling the server before marking the server as down and initiating failover. The default is 15 seconds, the range is 5-120 seconds.

**Example:**

```bash
hostname(cfg-scansafe)# health-check application timeout 20
```

Step 5  
Configure the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.

```bash
license hex_key
```

The authentication key is a 16-byte hexadecimal number. It can be a company or group key.

**Example:**

```bash
hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3
```

Step 6  
(Multiple context mode only.) Switch to each context where you want to use the service and enable it.

```bash
scansafe [license hex_key]
```

You can optionally enter a separate authentication key for each context. If you do not include an authentication key, the one configured for the system context is used.

**Example:**

```bash
hostname(config)# changeto context one
```
Examples

The following example configures a primary and backup server:

```
scansafe general-options
server primary ip 10.24.0.62 port 8080
server backup ip 10.10.0.7 port 8080
retry-count 7
health-check application
license 366C1D3F5CE67D33D3E9ACEC265261E5
```

The following sample configuration enables Cloud Web Security in context one with the default license and in context two with the license key override:

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
allocate-interface GigabitEthernet0/0.1
allocate-interface GigabitEthernet0/1.1
allocate-interface GigabitEthernet0/3.1
scansafe
config-url disk0:/one_ctx.cfg
!
context two
allocate-interface GigabitEthernet0/0.2
allocate-interface GigabitEthernet0/1.2
allocate-interface GigabitEthernet0/3.2
scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
config-url disk0:/two_ctx.cfg
!
```

Identify Whitelisted Traffic

If you use identity firewall or AAA rules, you can configure the ASA so that web traffic from specific users or groups that otherwise match the service policy rule is not redirected to the Cloud Web Security proxy server for scanning. This process is called “whitelisting” traffic.

You configure the whitelist in a ScanSafe inspection class map. You can use usernames and group names derived from both identity firewall and AAA rules. You cannot whitelist based on IP address or on destination URL.

When you configure your Cloud Web Security service policy rule, you refer to the class map in your policy. Although you can achieve the same results of exempting traffic based on user or group when you configure the traffic matching criteria (with ACLs) in the service policy rule, you might find it more straightforward to use a whitelist instead.
Procedure

Step 1  Create the class map: `class-map type inspect scansafe [match-all | match-any] class_map_name`

Where the `class_map_name` is the name of the class map. The `match-all` keyword is the default, and specifies that traffic must match all criteria to match the class map. The `match-any` keyword specifies that the traffic matches the class map if it matches at least one `match` statement. The CLI enters class-map configuration mode, where you can enter one or more `match` commands.

Example:

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
```

Step 2  Specify the whitelisted users and groups.

```
match [not] {[user username] [group groupname]}
```

The `match` keyword specifies a user or group to whitelist, or both.

The `match not` keyword specifies that the user or group should be filtered using Cloud Web Security. For example, if you whitelist the group “cisco,” but you want to scan traffic from users “johncrichton” and “aerynsun,” which are members of that group, you can specify `match not` for those users. Repeat this command to add as many users and groups as needed.

Example

The following example whitelists the same users and groups for the HTTP and HTTPS inspection policy maps:

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap-p)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```
Configure a Service Policy to Send Traffic to Cloud Web Security

Your service policy consists of multiple service policy rules, applied globally, or applied to each interface. Each service policy rule can either send traffic to Cloud Web Security (Match) or exempt traffic from Cloud Web Security (Do Not Match).

Create rules for traffic destined for the Internet. The order of these rules is important. When the ASA decides whether to forward or exempt a packet, the ASA tests the packet with 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 a rule at the beginning of a policy that explicitly Matches all traffic, no further statements are ever checked.

Before you begin

If you need to use a whitelist to exempt some traffic from being sent to Cloud Web Security, first create the whitelist so you can refer to it in your service policy rule.

Procedure

Step 1
Create the ScanSafe inspection policy maps. You need to define separate maps for HTTP and HTTPS.

a) Create the ScanSafe inspection policy map: `policy-map type inspect scansafe policy_map_name`

   Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

b) Enter parameters configuration mode.

   `hostname(config-pmap)# parameters`
   `hostname(config-pmap-p)#`

c) Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option:

   • `{http | https}`—The service type for this map. You can only specify one service type per map, so you need separate maps for HTTP and HTTPS.

   • `default {[user username] [group groupname]}`—(Optional.) The default user or group name, or both. If the ASA cannot determine the identity of the user coming into the ASA, then the default user and group is included in the HTTP request sent to Cloud Web Security. You can define policies in ScanCenter for this user or group name.

d) (Optional.) If you defined a whitelist, identify the class and use the `whitelist` command to mark it as a whitelist.

   `hostname(config-pmap-p)# class whitelist1`
   `hostname(config-pmap-c)# whitelist`

e) Repeat the process to create an inspection policy map for the other protocol, HTTP or HTTPS.

Step 2
Define the classes for the traffic you want to redirect to Cloud Web Security.
ACL matching is the most flexible way to define the class. However, if you want to send all HTTP/HTTPS traffic, you could instead use a port match in the class (match port tcp 80 and match port tcp 443). The following procedure describes an ACL match.

a) Create ACLs (access-list extended command) to identify the traffic you want to send to Cloud Web Security. You must create separate ACLs for HTTP and HTTPS traffic. Because Cloud Web Security works on HTTP/HTTPS traffic only, any other traffic defined in the ACL is ignored.

A permit ACE sends matching traffic to Cloud Web Security. A deny ACE exempts traffic from the service policy rule, so it is not sent to Cloud Web Security. Use tcp for the protocol, and identify the port (80 for HTTP, 443 for HTTPS).

When creating your ACLs, consider how you can match appropriate traffic that is destined for the Internet, but not match traffic that is destined for other internal networks. For example, to prevent inside traffic from being sent to Cloud Web Security when the destination is an internal server on the DMZ, be sure to add a deny ACE to the ACL that exempts traffic to the DMZ.

FQDN network objects might be useful in exempting traffic to specific servers. You can also use identity firewall user arguments and Cisco Trustsec security groups to help identify traffic. Note that Trustsec security group information is not sent to Cloud Web Security; you cannot define policy based on security group.

Create as many ACLs as needed for your policy. You can apply redirection to any number of traffic classes.

Example:

The following example shows how to exempt HTTP traffic to two servers, but include the remaining traffic. You would create a duplicate ACL for HTTPS traffic, where you simply change the port to 443.

```
hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com

hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
```

b) Create a traffic class for each ACL you defined.

```
hostname(config)# class-map class_name
hostname(config-cmap)# match access-list acl_name

Example:

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS
```

Step 3 Create or edit the policy map to redirect the traffic to Cloud Web Security.

a) Add or edit a policy map that sets the actions to take with the class map traffic: policy-map name
In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. You can only apply one policy to each interface or globally.

**Example:**

```
hostname(config)# policy-map global_policy
```

b) Identify one of the traffic class maps you created for Cloud Web Security inspection: **class name**

**Example:**

```
hostname(config-pmap)# class cws_class1
```

c) Configure ScanSafe inspection for the class.

```
inspect scansafe scansafe_policy_map [fail-open | fail-close]
```

Where:

- `scansafe_policy_map` is the ScanSafe inspection policy map. Ensure that you match the protocols in the class and policy maps (both HTTP or HTTPS).
- Specify **fail-open** to allow traffic to pass through the ASA if the Cloud Web Security servers are unavailable.
- Specify **fail-close** to drop all traffic if the Cloud Web Security servers are unavailable. **fail-close** is the default.

**Example:**

```
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
```

**Note** If you are editing the default global policy (or any in-use policy) to use a different ScanSafe inspection policy map, you must remove the ScanSafe inspection with the `no inspect scansafe` command, and then re-add it with the new inspection policy map name.

d) Add the class for the other protocol and enable inspection. If you have additional classes, add them also.

```
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
```

**Step 4** If you are editing an existing service policy (such as the default global policy called `global_policy`), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Example:**

```
hostname(config)# service-policy global_policy global
```
The **global** keyword applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

### Example

The following example configures two classes: one for HTTP and one for HTTPS. Each ACL exempts traffic to www.cisco.com and to tools.cisco.com, and to the DMZ network, for both HTTP and HTTPS. All other traffic is sent to Cloud Web Security, except for traffic from several whitelisted users and groups. The policy is then applied to the inside interface.

```config
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq 80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object dmz_network eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config-cmap)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
```
Configure the User Identity Monitor

When you use identity firewall, the ASA only downloads user identity information from the AD server for users and groups included in active ACLs. The ACL must be used in a feature such as an access rule, AAA rule, service policy rule, or other feature to be considered active.

For example, although you can configure your Cloud Web Security service policy rule to use an ACL with users and groups, thus activating any relevant groups, it is not required. You could use an ACL based entirely on IP addresses.

Because Cloud Web Security can base its ScanCenter policy on user identity, you might need to download groups that are not part of an active ACL to get full identity firewall coverage for all your users. The user identity monitor lets you download group information directly from the AD agent.

Note

The ASA can only monitor a maximum of 512 groups, including those configured for the user identity monitor and those monitored through active ACLs.

Procedure

Step 1

Identify the groups that you want to use in ScanCenter policies that are not already used in active ACLs. If necessary, create local user group objects.

Step 2

Download the group information from the AD agent.

```
user-identity monitor {user-group [domain-name]\|group-name | object-group-user object-group-name}
```

Where:

- `user-group`—Specifies a group name defined in the AD server.
- `object-group-user`—The name of a local object created by the `object-group user` command. This group can include multiple groups.

Example:

```
hostname(config)# user-identity monitor user-group CISCO\\Engineering
```

Configure the Cloud Web Security Policy

After you configure the ASA service policy rules, launch the ScanCenter Portal to configure Web content scanning, filtering, malware protection services, and reports.

Go to: https://scancenter.scansafe.com/portal/admin/login.jsp.
For more information, see the Cisco ScanSafe Cloud Web Security Configuration Guides:

Monitoring Cloud Web Security

To monitor Cloud Web Security, use the following commands:

- **show scansafe server**
  Shows the status of the server, whether it is the currently active server, the backup server, or unreachable.

  ```
  hostname# show scansafe server
  hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
  hostname# Backup: proxy137.scansafe.net (80.254.152.99)
  ```

- **show scansafe statistics**
  Shows information about Cloud Web Security activity, such as the number of connections redirected to the proxy server, the number of current connections being redirected, and the number of white listed connections:

  ```
  hostname# show scansafe statistics
  Current HTTP sessions : 0
  Current HTTPS sessions : 0
  Total HTTP Sessions : 0
  Total HTTPS Sessions : 0
  Total Fail HTTP sessions : 0
  Total Fail HTTPS sessions : 0
  Total Bytes In : 0 Bytes
  Total Bytes Out : 0 Bytes
  HTTP session Connect Latency in ms (min/max/avg) : 0/0/0
  HTTPS session Connect Latency in ms (min/max/avg) : 0/0/0
  ```

- **show service policy inspect scansafe**
  Shows the number of connections that are redirected or white listed by a particular policy.

  ```
  hostname(config)# show service-policy inspect scansafe
  Global policy:
    Service-policy: global_policy
      Class-map: inspection_default
    Interface inside:
      Service-policy: scansafe-pmap
        Class-map: scansafe-cmap
          Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0, v6-fail-close 0
    Number of whitelisted connections: 0
    Number of connections allowed without scansafe inspection because of "fail-open" config: 0
    Number of connections dropped because of "fail-close" config: 0
    Number of HTTP connections inspected: 0
    Number of HTTPS connections inspected: 0
    Number of HTTP connections dropped because of errors: 0
    Number of HTTPS connections dropped because of errors: 0
  ```

- **show conn scansafe**
Shows all Cloud Web Security connections, as noted by the capital Z flag.

You can determine if a user’s traffic is being redirected to the proxy servers by accessing the following URL from the client machine. The page will show a message indicating whether the user is currently using the service.

http://Whoami.scansafe.net

Examples for Cisco Cloud Web Security

Following are some examples for configuring Cloud Web Security.

Cloud Web Security Example with Identity Firewall

The following example shows a complete configuration for Cisco Cloud Web Security in single context mode, including the optional configuration for identity firewall.

Procedure

Step 1  Configure Cloud Web Security on the ASA.

hostname(config)# scansafe general-options
hostname(config)# server primary ip 192.168.115.225
hostname(config)# retry-count 5
hostname(config)# license 366C1D3F5CE67D33D3E9ACEC265261E5

Step 2  Configure identity firewall settings.

Because groups are a key feature of ScanCenter policies, you should consider enabling the identity firewall if you are not already using it. However, identity firewall is optional. The following example shows how to define the Active Directory (AD) server, the AD agent, configure identity firewall settings, and enable the user identity monitor for a few groups.

aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
  server-port 389
  ldap-base-dn DC=ASASCANLAB,DC=local
  ldap-scope subtree
  ldap-login-password *****
  ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
  server-type microsoft
  aaa-server adagent protocol radius
    ad-agent-mode
    aaa-server adagent (inside) host 192.168.116.220
    key *****
    user-identity domain ASASCANLAB aaa-server AD
    user-identity default-domain ASASCANLAB
    user-identity action netbios-response-fail remove-user-ip
    user-identity poll-import-user-group-timer hours 1
    user-identity ad-agent aaa-server adagent
    user-identity user-not-found enable
    user-identity monitor user-group ASASCANLAB\GROUP1
Step 3  (Optional) Configure a whitelist.

If there are specific users or groups you would like to exempt from Cloud Web Security filtering, you can create a whitelist.

```plaintext
class-map type inspect scansafe match-any whiteListCmap
  match user LOCAL\user1
```

Step 4  Configure ACLs.

We recommend that you split the traffic by creating separate HTTP and HTTPS class maps so that you know how many HTTP and HTTPS packets have gone through.

Then, if you need to troubleshoot you can run debug commands to distinguish how many packets have traversed each class map and find out if you are pushing through more HTTP or HTTPS traffic:

```plaintext
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

Step 5  Configure class maps.

```plaintext
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

hostname(config)# class-map cmap-https
hostname(config-cmap)# match access-list https
```

Step 6  Configure inspection policy maps.

```plaintext
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist

hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstраффic
hostname(config-pmap-p)# https
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist
```

Step 7  Configure policy maps.

The following example creates unique policy maps for Cloud Web Security traffic.

```plaintext
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
```
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close

Alternatively, you can add the classes to the default global_policy to have redirection enabled for all interfaces. Ensure that you add the classes to global_policy rather than applying a new policy map globally, or you will remove the default protocol inspections that are part of the default global policy.

hostname(config)# policy-map global_policy
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close

**Step 8**

Configure service policy.

If you created a separate policy map for Cloud Web Security, the following example shows how to apply it to an interface. If you instead added the classes to the global_policy map, you are finished; you do not need to enter the service-policy command.

hostname(config)# service-policy pmap-webtraffic interface inside

---

**Active Directory Integration Example for Identity Firewall**

The following is an end-to-end example configuration for Active Directory integration. This configuration enables the identity firewall.

**Procedure**

**Step 1**

Configure the Active Directory Server Using LDAP.

The following example shows how to configure the Active Directory server on your ASA using LDAP:

hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1

**Step 2**

Configure the Active Directory Agent Using RADIUS.

The following example shows how to configure the Active Directory Agent on your ASA using RADIUS:

hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent

Step 3  
(On the AD Agent server.) Create the ASA as a Client on the AD Agent Server.  
The following example shows how to create the ASA as a client on the Active Directory agent server:

c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123

Step 4  
(On the AD Agent server.) Create a Link Between the AD Agent and DCs.  
The following example shows how to create a link between the Active Directory Agent and all DCs for which you want to monitor logon/logoff events:

c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC -domain W2K3DC.asascanlab.local -user administrator -password Password1  
c:\IBF\CLI\adacfg.exe dc list

Running the last command should show the status as “UP.”

For the AD Agent to monitor logon/logoff events, you need to ensure that these are logged on all DCs that are actively being monitored. To do this, choose:

Start > Administrative Tools > Domain Controller Security Policy  
Local policies > Audit Policy > Audit account logon events (success and failure)

Step 5  
(Back on the ASA.) Test the AD Agent.  
The following example shows how to configure the test Active Directory Agent so that it can communicate with the ASA:

hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220  
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)  
INFO: Ad-agent Successful

See also the following command: show user-identity ad-agent.

Step 6  
Configure the Identity Options on the ASA.  
The following example shows how to configure the identity options on the ASA:

hostname(config)# user-identity domain ASASCANLAB aaa-server AD  
hostname(config)# user-identity default-domain ASASCANLAB

Step 7  
Configure the User Identity Options and Enabling Granular Reporting.  
The following example shows how to configure the user identity options that send user credentials to the ASA and enable granular user reporting from the proxy server:

hostname(config)# user-identity inactive-user-timer minutes 60  
hostname(config)# user-identity action netbios-response-fail remove-user-ip  
hostname(config)# user-identity user-not-found enable  
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download

There are two download modes with Identify Firewall: Full download and On-demand.

- **Full download**—Whenever a user logs into the network, the IDFW tells the ASA the User identity immediately (recommended on the ASA 5512-X and above).

- **On-demand**—Whenever a user logs into the network, the ASA requests the user identity from AD.

If you are using more than one domain, then enter the following command:

hostname(config)# user-identity domain OTHERDOMAINNAME

**Step 8**

Monitor the Active Directory Groups.

The following example shows how to configure Active Directory groups to be monitored:

hostname(config)# user-identity monitor user-group ASASCANLAB\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\GROUPNAME3

Remember to save your configuration once the above is completed.

**Step 9**

Download the Entire Active-User Database from the Active Directory Server.

The following command updates the specified import user group database by querying the Active Directory server immediately without waiting for the expiration of poll-import-user-group-timer:

hostname(config)# user-identity update import-user

**Step 10**

Download the Database from the AD Agent.

The following example shows how to manually start the download of the database from the Active Directory Agent if you think the user database is out of sync with Active Directory:

hostname(config)# user-identity update active-user-database

**Step 11**

Show a List of Active Users.

hostname# show user-identity user active list detail
# History for Cisco Cloud Web Security

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Web Security</td>
<td>9.0(1)</td>
<td>This feature was introduced. Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. We introduced or modified the following commands: **class-map type inspect scansafe, default user group, http[s] (parameters), inspect scansafe, license, match user group, policy-map type inspect scansafe, retry-count, scansafe, scansafe general-options, server {primary</td>
</tr>
<tr>
<td>Application layer health checking for Cisco Cloud Web Security.</td>
<td>9.6(2)</td>
<td>You can now configure Cisco Cloud Web Security to check the health of the Cloud Web Security application when determining if the server is healthy. By checking application health, the system can fail over to the backup server when the primary server responds to the TCP three-way handshake but cannot process requests. This ensures a more reliable system. We added the following commands: <strong>health-check application url, health-check application timeout.</strong></td>
</tr>
</tbody>
</table>
PART II

Firewall Services for Virtual Environments

• Attribute-Based Access Control, on page 189
CHAPTER 10

Attribute-Based Access Control

Attributes are customized network objects for use in your configuration. You can define and use them in Cisco ASA configurations to filter traffic associated with one or more virtual machines in an VMware ESXi environment managed by VMware vCenter. Attributes allow you to define access control lists (ACLs) to assign policies to traffic from groups of virtual machines sharing one or more attributes. You assign attributes to virtual machines within the ESXi environment and configure an attribute agent, which connects to vCenter or a single ESXi host using HTTPS. The agent then requests and retrieves one or more bindings which correlate specific attributes to the primary IP address of a virtual machine.

Attribute-based access control is supported on all hardware platforms, and on all ASAv platforms running on ESXi, KVM, or HyperV hypervisors. Attributes can only be retrieved from virtual machines running on an ESXi hypervisor.

- Guidelines for Attribute-Based Network Objects, on page 189
- Configure Attribute-Based Access Control, on page 190
- Monitoring Attribute-Based Network Objects, on page 197
- History for Attribute-Based Access Control, on page 198

Guidelines for Attribute-Based Network Objects

IPv6 Guidelines

- IPv6 addresses not supported by vCenter for host credentials.
- IPv6 is supported for virtual machine bindings where the primary IP address of the virtual machine is an IPv6 address.

Additional Guidelines and Limitations

- Multi-context mode is not supported. Attribute-based network objects are supported for single-mode context only.
- Attribute-based network objects support binding to the virtual machine’s primary address only. Binding to multiple vNICs on a single virtual machine is not supported.
- Attribute-based network objects may only be configured for objects used for access groups. Network objects for other features (NAT, etc.) are not supported.
Configure Attribute-Based Access Control

The following procedure provides a general sequence for implementing attribute-based access control on managed virtual machines in a VMware ESXi environment.

Procedure

Step 1  Assign custom attribute types and values to your managed virtual machines. See Configure Attributes for vCenter Virtual Machines, on page 190.

Step 2  Configure an attribute agent to connect to your vCenter Server or ESXi host. See Configure a VM Attribute Agent, on page 192.

Step 3  Configure attribute-based network objects needed for your deployment scheme. See Configure Attribute-Based Network Objects, on page 194.

Step 4  Configure the access control lists and rules. See Configure Access Control Using Attribute-Based Network Objects, on page 195.

Configure Attributes for vCenter Virtual Machines

You assign custom attribute types and values to virtual machines, and associate these attributes to network objects. You can then use these attribute-based network objects to apply ACLs to a set of virtual machines with common user-defined characteristics. For example, you could isolate developer build machines from test machines, or group virtual machines by project and/or location. For the ASA to monitor virtual machines using attributes, you need to make the attributes available to vCenter from the managed virtual machines. You do this by inserting a formatted text file into the Notes field, which is found on the Summary page of virtual machines in vCenter.

You can see the Notes field in the following figure.
To specify custom attributes, you copy a properly formatted XML file into the Notes field for the virtual machine. The format of the file is:

```xml
<CustomAttributes>
    <Attribute type='attribute-type' value='attribute-value'/>
    ...
</CustomAttributes>
```

A single virtual machine may have multiple attributes defined by repeating the second line above. Note that each line must identify a unique attribute type. If the same attribute type is defined with multiple attribute values, each binding update for that attribute type will overwrite the previous one.

For string attribute values, the value associated with the object definition must be an exact match to the value reported to vCenter by the virtual machine. For example, an attribute value Build Machine does not match the annotation value build machine on the virtual machine. A binding would not be added to the host-map for this attribute.

You can define multiple unique attribute types in a single file.
Procedure

Step 1
Select the virtual machine from your vCenter inventory.

Step 2
Click the **Summary** tab for the virtual machine.

Step 3
In the **Notes** field, click the **Edit** link.

Step 4
Paste the custom attributes text file into the **Edit Notes** box. The text file should follow the XML template format:

**Example:**

```xml
<CustomAttributes>
  <Attribute type='attribute-type' value='attribute-value'/>
  ...
</CustomAttributes>
```

Step 5
Click **OK**.

---

**Example**

The following example shows a properly formatted XML text file that defines custom attributes for 'role' and 'project' that you can apply to virtual machines:

```xml
<CustomAttributes>
  <Attribute type='role' value='Developer'/>
  <Attribute type='project' value='Alpha'/>
</CustomAttributes>
```

**Configure a VM Attribute Agent**

You configure a VM attribute agent to communicate with vCenter or a single ESXi host. When you assign attributes to virtual machines within the VMware environment, the attribute agent sends a message to vCenter indicating which attributes have been configured, and vCenter responds with a binding update for every virtual machine where a matching attribute type is configured.

The VM attribute agent and vCenter exchange binding updates as follows:

- If the agent issues a request containing a new attribute type, vCenter responds with a binding update for every virtual machine where the attribute type is configured. After that point, vCenter only issues a new binding when an attribute value is added or changed.

- If a monitored attribute changes for one or more virtual machines, a binding update message is received. Each binding message is identified by the IP address of the virtual machine reporting the attribute value.

- If multiple attributes are being monitored by a single agent, a single binding update contains the current value of all monitored attributes for each virtual machine.

- If a specific attribute being monitored by the agent is not configured on a virtual machine, the binding will contain an empty attribute value for that virtual machine.

- If a virtual machine has not been configured with any monitored attributes, vCenter does not send a binding update.
Each attribute agent communicates with exactly one vCenter or ESXi host. A single ASA may have multiple attribute agents defined, each communicating with a different vCenter, or one or more communicating with the same vCenter.

**Procedure**

**Step 1** Create the VM attribute agent to communicates with vCenter: `attribute source-group agent-name type agent-type`

**Example:**

```plaintext
hostname(config)# attribute source-group VMAgent type esxi
```

The `agent-name` argument specifies the VM attribute agent name. The `type` argument is the type of attribute agent.

**Note** Currently ESXi is the only supported agent type.

**Step 2** Configure your vCenter host credentials: `host ip-address username ESXi-username password ESXi-password`

**Example:**

```plaintext
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

**Step 3** Configure keepalive settings for vCenter communication: `keepalive retry-interval interval retry-count count`

**Example:**

```plaintext
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

The default keepalive timer values are 3 retries at 30-second intervals.

**Step 4** Examine the VM attribute agent configuration: `show attribute source-group agent-name`

**Example:**

```plaintext
hostname(config-attr)# sh attribute source-group VMAgent

Attribute agent VMAgent
Agent type: ESXi
Agent state: Inactive
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
```

The *Agent State* remains inactive until you configure a network object and specify attributes to associate with the object.

**Step 5** Exit from the attribute configuration mode: `exit`

**Example:**
Configure Attribute-Based Network Objects

Attribute-based network objects filter traffic according to attributes associated with one or more virtual machines in a VMware ESXi environment. You can define access control lists (ACLs) to assign policies to traffic from groups of virtual machines sharing one or more attributes.

For example, you can configure access rules that permit machines with an engineering attribute to access machines with an eng_lab attribute. A network administrator can add or remove engineering machines and lab servers while the security policy managed by the security administrator continues to work automatically without manual updates to the access rules.

Procedure

Step 1 Enable object group search: object-group-search access-control

Example:

```
hostname(config)# object-group-search access-control
```

You must enable object-group-search to configure attribute-based network objects.

Step 2 Create or edit an attribute-based network object using the object name: object network object-id

Example:

```
hostname(config)# object network dev
```

Step 3 Specify an agent, attribute type, and attribute value to associate with the object: attribute agent-name attribute-type attribute-value

Example:

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

The agent-name specifies the VM attribute agent; see Configure a VM Attribute Agent. If you configure an attribute-based network object to use an attribute agent which has not been configured, a placeholder agent is automatically created with no credentials and default keepalive values. This agent remains in the "No credentials available" state until host credentials are supplied using the host subcommand.

Together, the attribute-type and attribute-value pair define a unique attribute. The attribute-type is an arbitrary string and must include the custom, prefix. If you define the same attribute type more than once with multiple attribute values, the last value defined overwrites the previous one.
Examples

The following example creates the attribute-based network object *dev* for a development group, with a role of 'Developer'. The VM attribute agent communicates with vCenter and returns all of the virtual machine bindings that match the attribute `custom.role`:

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

The following example creates the attribute-based network object *test* for a test group, with a role of 'Automation'. The VM attribute agent communicates with vCenter and returns all of the virtual machine bindings that match the attribute `custom.role`. Note that this is the same list of virtual machines as the previous example:

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

The following example creates the attribute-based network object *project* for a project group, with a role of 'Alpha'. The VM attribute agent communicates with vCenter and returns all of the virtual machine bindings that match the attribute `custom.project`. Note that some machines overlap more than one attribute:

```
hostname(config)# object network project
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

The following example shows a VM attribute agent in active status with pending attribute requests:

```
hostname(config-attr)# show attribute source-group VMAgent

Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attribute requests pending:
    'custom.project'
    'custom.role'
```

Configure Access Control Using Attribute-Based Network Objects

You can use attribute-based network objects when you define access control lists (ACLs) to traffic from groups of virtual machines sharing one or more attributes. Access lists are made up of one or more access control entries (ACEs). An ACE is a single entry in an access list that specifies a permit or deny rule (to forward or drop the packet). Typically a permit or deny rule is applied to a protocol, to a source and destination IP address or network, and, optionally, to the source and destination ports.

When you use attribute-based network objects, you can replace source and/or destination IP addresses with these objects. As virtual machines are deployed, moved, or retired, attributes can be updated on the virtual machines while the assigned access control policies can remain in effect without configuration changes.
For complete information on all of the available options for ACLs, see Configure ACLs, on page 26.

**Procedure**

**Step 1**
Create and configure an extended ACL entry (ACE) using attribute-based network objects:

```
access-list access_list_name extended {deny | permit} protocol_argument object source_object_name object dest_object_name
```

**Example:**

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

**Note**  Repeat as needed for your policies.

The options are:

- `access_list_name`—The name of the new or existing ACL.
- Permit or Deny—The `deny` keyword denies or exempts a packet if the conditions are matched. The `permit` keyword permits or includes a packet if the conditions are matched.
- Protocol—The `protocol_argument` specifies the IP protocol:
  - `name` or `number`—Specifies the protocol name or number. Specify `ip` to apply to all protocols.
  - `object-group protocol_grp_id`—Specifies a protocol object group created using the `object-group protocol` command.
- Source Object—`object` specifies an attribute-based network object created using the `object network` command. The `source_object_name` specifies the object from which the packet is being sent.
- Destination Object—`object` specifies an attribute-based network object created using the `object network` command. The `dest_object_name` specifies the object to which the packet is being sent.

**Step 2**
Bind the ACL to an interface or apply it globally:

```
access-group access_list_name {in interface interface_name | global}
```

**Example:**

```
hostname(config)# access-group lab-access in interface inside
```

For an interface-specific access group:

- Specify the extended ACL name. You can configure one `access-group` command per ACL type per interface.
- The `in` keyword applies the ACL to inbound traffic.
- Specify the `interface` name.

For a global access group, specify the `global` keyword to apply the extended ACL to the inbound direction of all interfaces.
Example

The following example shows how to apply an attribute-based extended ACL globally:

```bash
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
```

```bash
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0) 0x64a1be76
access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0) 0x64a1be76
```

Monitoring Attribute-Based Network Objects

To monitor attribute-based network objects, enter the following commands:

- **show attribute host-map**
  Displays attribute bindings for a given attribute's agent, type, and value.

- **show attribute object-map**
  Displays the object-to-attribute bindings.

- **show attribute source-group**
  Displays the configured VM attribute agents.

Examples

The following example shows a map of the host-to-attribute bindings:

```bash
hostname# show attribute host-map /all
```

**IP Address-Attribute Bindings Information**

<table>
<thead>
<tr>
<th>Source/Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMAgent.custom.project</td>
<td>'Alpha'</td>
</tr>
<tr>
<td>10.15.28.34</td>
<td></td>
</tr>
<tr>
<td>10.15.28.32</td>
<td></td>
</tr>
<tr>
<td>10.15.28.31</td>
<td></td>
</tr>
<tr>
<td>10.15.28.33</td>
<td></td>
</tr>
<tr>
<td>VMAgent.custom.role</td>
<td>'Automation'</td>
</tr>
<tr>
<td>10.15.27.133</td>
<td></td>
</tr>
<tr>
<td>10.15.27.135</td>
<td></td>
</tr>
<tr>
<td>10.15.27.134</td>
<td></td>
</tr>
<tr>
<td>VMAgent.custom.role</td>
<td>'Developer'</td>
</tr>
<tr>
<td>10.15.28.34</td>
<td></td>
</tr>
<tr>
<td>10.15.28.12</td>
<td></td>
</tr>
<tr>
<td>10.15.28.31</td>
<td></td>
</tr>
</tbody>
</table>
The following examples show the object-to-attribute bindings:

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information
Object Source/Attribute Value
dev VMAgent.custom.role 'Developer'
test VMAgent.custom.role 'Automation'
project VMAgent.custom.project 'Alpha'
```

The following example shows the attribute agent configuration:

```
hostname# show attribute source-group
Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attributes being monitored:
  'custom.role' (2)
```

## History for Attribute-Based Access Control

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| Support for Attribute-Based Network Objects | 9.7.(1) | You can now control network access using virtual machine attributes in addition to traditional network characteristics such as IP addresses, protocols, and ports. The virtual machines must be in a VMware ESXi environment. We introduced the following commands: **object network attribute**
**attribute agent-name attribute-type attribute-value**
**attribute source-group agent-name type agent-type**
**host ip-address username ESXi-username password ESXi-password keepalive retry-interval interval retry-count count** |
| Remove support for VM attribute-based network objects from ASA 5506-X (all models), 5508-X, 5512-X, 5516-X. | 9.10(1) | You can no longer use VM-attribute based network objects on the following platforms: ASA 5506-X (all models), 5508-X, 5512-X, 5516-X. |
PART III

Network Address Translation

• Network Address Translation (NAT), on page 201
• NAT Examples and Reference, on page 249
Network Address Translation (NAT)

The following topics explain Network Address Translation (NAT) and how to configure it.

- Why Use NAT?, on page 201
- NAT Basics, on page 202
- Guidelines for NAT, on page 206
- Dynamic NAT, on page 212
- Dynamic PAT, on page 219
- Static NAT, on page 230
- Identity NAT, on page 239
- Monitoring NAT, on page 243
- History for NAT, on page 244

Why Use NAT?

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private, not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of NAT is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security—Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions—Overlapping IP addresses are not a problem when you use NAT.
• Flexibility—You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.

• Translating between IPv4 and IPv6 (Routed mode only)—If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

Note
NAT is not required. If you do not configure NAT for a given set of traffic, that traffic will not be translated, but will have all of the security policies applied as normal.

NAT Basics

The following topics explain some of the basics of NAT.

NAT Terminology

This document uses the following terminology:

• Real address/host/network/interface—The real address is the address that is defined on the host, before it is translated. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the inside network would be the “real” network. Note that you can translate any network connected to the device, not just an inside network. Therefore if you configure NAT to translate outside addresses, “real” can refer to the outside network when it accesses the inside network.

• Mapped address/host/network/interface—The mapped address is the address that the real address is translated to. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the outside network would be the “mapped” network.

Note
During address translation, IP addresses configured for the device interfaces are not translated.

• Bidirectional initiation—Static NAT allows connections to be initiated bidirectionally, meaning both to the host and from the host.

• Source and destination NAT—For any given packet, both the source and destination IP addresses are compared to the NAT rules, and one or both can be translated/untranslated. For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address.

NAT Types

You can implement NAT using the following methods:
Network Address Translation

- Dynamic NAT—A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses, on a first come, first served basis. Only the real host can initiate traffic. See Dynamic NAT, on page 212.

- Dynamic Port Address Translation (PAT)—A group of real IP addresses are mapped to a single IP address using a unique source port of that IP address. See Dynamic PAT, on page 219.

- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See Static NAT, on page 230.

- Identity NAT—A real address is statically translated to itself, essentially bypassing NAT. You might want to configure NAT this way when you want to translate a large group of addresses, but then want to exempt a smaller subset of addresses. See Identity NAT, on page 239.

Network Object NAT and Twice NAT

You can implement address translation in two ways: network object NAT and twice NAT.

We recommend using network object NAT unless you need the extra features that twice NAT provides. It is easier to configure network object NAT, and it might be more reliable for applications such as Voice over IP (VoIP). (For VoIP, you might see a failure in the translation of indirect addresses that do not belong to either of the objects used in the rule.)

Network Object NAT

All NAT rules that are configured as a parameter of a network object are considered to be network object NAT rules. This is a quick and easy way to configure NAT for a network object. You cannot create these rules for a group object, however.

After you configure the network object, you can then identify the mapped address for that object, either as an inline address or as another network object or network object group.

When a packet enters an interface, both the source and destination IP addresses are checked against the network object NAT rules. The source and destination address in the packet can be translated by separate rules if separate matches are made. These rules are not tied to each other; different combinations of rules can be used depending on the traffic.

Because the rules are never paired, you cannot specify that sourceA/destinationA should have a different translation than sourceA/destinationB. Use twice NAT for that kind of functionality, where you can identify the source and destination address in a single rule.

Twice NAT

Twice NAT lets you identify both the source and destination address in a single rule. Specifying both the source and destination addresses lets you specify that sourceA/destinationA can have a different translation than sourceA/destinationB.
For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address. For example, if you configure static NAT with port address translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then you must specify the source ports to be translated (real: 23, mapped: 2323). You specify the source ports because you specified the Telnet server address as the source address.

The destination address is optional. If you specify the destination address, you can either map it to itself (identity NAT), or you can map it to a different address. The destination mapping is always a static mapping.

Comparing Network Object NAT and Twice NAT

The main differences between these two NAT types are:

- How you define the real address.
  - Network object NAT—You define NAT as a parameter for a network object. A network object names an IP host, range, or subnet so you can then use the object in the NAT configuration instead of the actual IP addresses. The network object IP address serves as the real address. This method lets you easily add NAT to network objects that might already be used in other parts of your configuration.
  - Twice NAT—You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network object; the network object or group is a parameter of the NAT configuration. The ability to use a network object group for the real address means that twice NAT is more scalable.

- How source and destination NAT is implemented.
  - Network Object NAT—Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.
  - Twice NAT—A single rule translates both the source and destination. A packet matches one rule only, and further rules are not checked. Even if you do not configure the optional destination address, a matching packet still matches one twice NAT rule only. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different translation than sourceA/destinationB.

- Order of NAT Rules.
  - Network Object NAT—Automatically ordered in the NAT table.
  - Twice NAT—Manually ordered in the NAT table (before or after network object NAT rules).

NAT Rule Order

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if
a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

*Table 9: NAT Rule Table*

<table>
<thead>
<tr>
<th>Table Section</th>
<th>Rule Type</th>
<th>Order of Rules within the Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>Twice NAT</td>
<td>Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1.</td>
</tr>
<tr>
<td>Section 2</td>
<td>Network Object NAT</td>
<td>If a match in section 1 is not found, section 2 rules are applied in the following order:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Static rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Dynamic rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Within each rule type, the following ordering guidelines are used:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.</td>
</tr>
<tr>
<td>Section 3</td>
<td>Twice NAT</td>
<td>If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.</td>
</tr>
</tbody>
</table>

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1/32 (static)
- 172.16.1.0/24 (dynamic) (object def)
- 172.16.1.0/24 (dynamic) (object abc)

The resultant ordering would be:
NAT Interfaces

Except for bridge group member interfaces, you can configure a NAT rule to apply to any interface (in other words, all interfaces), or you can identify specific real and mapped interfaces. You can also specify any interface for the real address, and a specific interface for the mapped address, or vice versa.

For example, you might want to specify any interface for the real address and specify the outside interface for the mapped address if you use the same private addresses on multiple interfaces, and you want to translate them all to the same global pool when accessing the outside.

Figure 17: Specifying Any Interface

However, the concept of “any” interface does not apply to bridge group member interfaces. When you specify “any” interface, all bridge group member interfaces are excluded. Thus, to apply NAT to bridge group members, you must specify the member interface. This could result in many similar rules where only one interface is different. You cannot configure NAT for the Bridge Virtual Interface (BVI) itself, you can configure NAT for member interfaces only.

Guidelines for NAT

The following topics provide detailed guidelines for implementing NAT.

Firewall Mode Guidelines for NAT

NAT is supported in routed and transparent firewall mode.

However, configuring NAT on bridge group member interfaces (interfaces that are part of a Bridge Group Virtual Interface, or BVI) has the following restrictions:
• When configuring NAT for the members of a bridge group, you specify the member interface. You cannot configure NAT for the bridge group interface (BVI) itself.

• When doing NAT between bridge group member interfaces, you must specify the real and mapped addresses. You cannot specify “any” as the interface.

• You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.

• You cannot translate between IPv4 and IPv6 networks (NAT64/46) when the source and destination interfaces are members of the same bridge group. Static NAT/PAT 44/66, dynamic NAT44/66, and dynamic PAT44 are the only allowed methods; dynamic PAT66 is not supported. However, you can do NAT64/46 between members of different bridge groups, or between a bridge group member (source) and standard routed interface (destination).

IPv6 NAT Guidelines

NAT supports IPv6 with the following guidelines and restrictions.

• For standard routed mode interfaces, you can also translate between IPv4 and IPv6.

• You cannot translate between IPv4 and IPv6 for interfaces that are members of the same bridge group. You can translate between two IPv6 or two IPv4 networks only. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.

• You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.

• For static NAT, you can specify an IPv6 subnet up to /64. Larger subnets are not supported.

• When using FTP with NAT46, when an IPv4 FTP client connects to an IPv6 FTP server, the client must use either the extended passive mode (EPSV) or extended port mode (EPRT); PASV and PORT commands are not supported with IPv6.

IPv6 NAT Recommendations

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices:

• NAT66 (IPv6-to-IPv6)—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only).

• NAT46 (IPv4-to-IPv6)—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (twice NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is by default an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.14 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after
the prefix, and a suffix of 0s is appended after the IPv4 address. You can also optionally translate the addresses net-to-net, where the first IPv4 address maps to the first IPv6 address, the second to the second, and so on.

- **NAT64 (IPv6-to-IPv4)**—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

## Additional Guidelines for NAT

- For interfaces that are members of a bridge group, you write NAT rules for the member interfaces. You cannot write NAT rules for the Bridge Virtual Interface (BVI) itself.

- *(Network Object NAT only.)* You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules for an object, you need to create multiple objects with different names that specify the same IP address. For example, `object network obj-10.10.10.1-01`, `object network obj-10.10.10.1-02`, and so on.

- If a VPN is defined on an interface, inbound ESP traffic on the interface is not subject to the NAT rules. The system allows the ESP traffic for established VPN tunnels only, dropping traffic not associated with an existing tunnel. This restriction applies to ESP and UDP ports 500 and 4500.

- If you define a site-to-site VPN on a device that is behind a device that is applying dynamic PAT, so that UDP ports 500 and 4500 are not the ones actually used, you must initiate the connection from the device that is behind the PAT device. The responder cannot initiate the security association (SA) because it does not know the correct port numbers.

- If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT configuration is used, you can clear the translation table using the `clear xlate` command in the device CLI. However, clearing the translation table disconnects all current connections that use translations.

  **Note**

  If you remove a dynamic NAT or PAT rule, and then add a new rule with mapped addresses that overlap the addresses in the removed rule, then the new rule will not be used until all connections associated with the removed rule time out or are cleared using the `clear xlate` command. This safeguard ensures that the same address is not assigned to multiple hosts.

- When translating SCTP traffic, use static network object NAT only. Dynamic NAT/PAT is not allowed. Although you can configure static twice NAT, this is not recommended because the topology of the destination part of the SCTP association is unknown.

- Objects and object groups used in NAT cannot be undefined; they must include IP addresses.

- You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.

- *(Twice NAT only.)* When using `any` as the source address in a NAT rule, the definition of “any” traffic (IPv4 vs. IPv6) depends on the rule. Before the ASA performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the ASA can determine the value of `any` in a NAT rule. For example, if you configure a rule from “any” to an IPv6 server, and that server was mapped from an IPv4 address, then `any` means “any IPv6 traffic.” If you configure a rule from “any” to “any,” and
you map the source to the interface IPv4 address, then any means “any IPv4 traffic” because the mapped interface address implies that the destination is also IPv4.

• You can use the same mapped object or group in multiple NAT rules.

• The mapped IP address pool cannot include:
  • The mapped interface IP address. If you specify “any” interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), specify the interface name instead of the interface address.
  • The failover interface IP address.
  • (Transparent mode.) The management IP address.
  • (Dynamic NAT.) The standby interface IP address when VPN is enabled.
  • Existing VPN pool addresses.

• Avoid using overlapping addresses in static and dynamic NAT policies. For example, with overlapping addresses, a PPTP connection can fail to get established if the secondary connection for PPTP hits the static instead of dynamic xlate.

• For application inspection limitations with NAT or PAT, see Default Inspections and NAT Limitations, on page 311.

• The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. See Routing NAT Packets, on page 260 for more information.

• If you enable the arp permit-nonconnected command, the system does not respond to ARP requests if the mapped address is not part of any connected subnet and you also do not specify the mapped interface in the NAT rule (that is, you specify "any" interface). To resolve this problem, specify the mapped interface.

• If you specify a destination interface in a rule, then that interface is used as the egress interface rather than looking up the route in the routing table. However, for identity NAT, you have the option to use a route lookup instead.

• You can improve system performance and reliability by using the transactional commit model for NAT. See the basic settings chapter in the general operations configuration guide for more information. Use the asp rule-engine transactional-commit nat command.

---

**Network Object NAT Guidelines for Mapped Address Objects**

For dynamic NAT, you must use an object or group for the mapped addresses. For the other NAT types, you can use an object or group, or you have the option of using inline addresses. Network object groups are particularly useful for creating a mapped address pool with discontinuous IP address ranges or multiple hosts or subnets. Use the object network and object-group network commands to create the objects.

Consider the following guidelines when creating objects for mapped addresses.

• A network object group can contain objects or inline addresses of either IPv4 or IPv6 addresses. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

• See Additional Guidelines for NAT, on page 208 for information about disallowed mapped IP addresses.
• Dynamic NAT:
  • You cannot use an inline address; you must configure a network object or group.
  • The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.
  • If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.

• Dynamic PAT (Hide):
  • Instead of using an object, you can optionally configure an inline host address or specify the interface address.
  • If you use an object, the object or group cannot contain a subnet. The object must define a host, or for a PAT pool, a range. The group (for a PAT pool) can include hosts and ranges.

• Static NAT or Static NAT with port translation:
  • Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).
  • If you use an object, the object or group can contain a host, range, or subnet.

• Identity NAT
  • Instead of using an object, you can configure an inline address.
  • If you use an object, the object must match the real addresses you want to translate.

**Twice NAT Guidelines for Real and Mapped Address Objects**

For each NAT rule, configure up to four network objects or groups for:

- Source real address
- Source mapped address
- Destination real address
- Destination mapped address

Objects are required unless you specify the *any* keyword inline to represent all traffic, or for some types of NAT, the *interface* keyword to represent the interface address. Network object groups are particularly useful for creating a mapped address pool with discontinuous IP address ranges or multiple hosts or subnets. Use the `object network` and `object-group network` commands to create the objects.

Consider the following guidelines when creating objects for twice NAT:

- A network object group can contain objects or inline addresses of either IPv4 or IPv6 addresses. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
- See Additional Guidelines for NAT, on page 208 for information about disallowed mapped IP addresses.
- Source Dynamic NAT:
• You typically configure a larger group of real addresses to be mapped to a smaller group.

• The mapped object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.

• If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and the host IP addresses are used as a PAT fallback.

• Source Dynamic PAT (Hide):
  • If you use an object, the object or group cannot contain a subnet. The object must define a host, or for a PAT pool, a range. The group (for a PAT pool) can include hosts and ranges.

• Source Static NAT or Static NAT with port translation:
  • The mapped object or group can contain a host, range, or subnet.
  • The static mapping is typically one-to-one, so the real addresses have the same quantity as the mapped addresses. You can, however, have different quantities if desired.

• Source Identity NAT
  • The real and mapped objects must match. You can use the same object for both, or you can create separate objects that contain the same IP addresses.

• Destination Static NAT or Static NAT with port translation (the destination translation is always static):
  • Although the main feature of twice NAT is the inclusion of the destination IP address, the destination address is optional. If you do specify the destination address, you can configure static translation for that address or just use identity NAT for it. You might want to configure twice NAT without a destination address to take advantage of some of the other qualities of twice NAT, including the use of network object groups for real addresses, or manually ordering of rules. For more information, see Comparing Network Object NAT and Twice NAT, on page 204.

  • For identity NAT, the real and mapped objects must match. You can use the same object for both, or you can create separate objects that contain the same IP addresses.

  • The static mapping is typically one-to-one, so the real addresses have the same quantity as the mapped addresses. You can, however, have different quantities if desired.

  • For static interface NAT with port translation (routed mode only), you can specify the interface keyword instead of a network object/group for the mapped address.

**Twice NAT Guidelines for Service Objects for Real and Mapped Ports**

You can optionally configure service objects for:

• **Source real port (Static only) or Destination real port**

• **Source mapped port (Static only) or Destination mapped port**

Use the `object service` command to create the objects.

Consider the following guidelines when creating objects for twice NAT.
• NAT supports TCP, UDP, and SCTP only. When translating a port, be sure the protocols in the real and mapped service objects are identical (for example, both TCP). Although you can configure static twice NAT rules with SCTP port specifications, this is not recommended, because the topology of the destination part of the SCTP association is unknown. Use static object NAT instead for SCTP.

• The “not equal” (neq) operator is not supported.

• For identity port translation, you can use the same service object for both the real and mapped ports.

• Source Dynamic NAT—Source Dynamic NAT does not support port translation.

• Source Dynamic PAT (Hide)—Source Dynamic PAT does not support port translation.

• Source Static NAT, Static NAT with port translation, or Identity NAT—A service object can contain both a source and destination port; however, you should specify either the source or the destination port for both service objects. You should only specify both the source and destination ports if your application uses a fixed source port (such as some DNS servers); but fixed source ports are rare. For example, if you want to translate the port for the source host, then configure the source service.

• Destination Static NAT or Static NAT with port translation (the destination translation is always static)—For non-static source NAT, you can only perform port translation on the destination. A service object can contain both a source and destination port, but only the destination port is used in this case. If you specify the source port, it will be ignored.

Dynamic NAT

The following topics explain dynamic NAT and how to configure it.

About Dynamic NAT

Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool typically includes fewer addresses than the real group. When a host you want to translate accesses the destination network, NAT assigns the host an IP address from the mapped pool. The translation is created only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, even if the connection is allowed by an access rule.

For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

The following figure shows a typical dynamic NAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back.
Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

  Use PAT or a PAT fall-back method if this event occurs often because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool, and routable addresses may not be available in large quantities.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.
• Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

See Default Inspections and NAT Limitations, on page 311 for more information about NAT and PAT support.

Configure Dynamic Network Object NAT

This section describes how to configure network object NAT for dynamic NAT.

Procedure

Step 1  Create a host or range network object (object network command), or a network object group (object-group network command), for the mapped addresses.

• The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.

• If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.

Step 2  Create or edit the network object for which you want to configure NAT: object network obj_name

Example:

hostname(config)# object network my-host-obj1

Step 3  (Skip when editing an object that has the right address.) Define the real IPv4 or IPv6 addresses that you want to translate.

• host {IPv4_address | IPv6_address}—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.

• subnet {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

• range start_address end_address—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

Example:

hostname(config-network-object)# host 10.2.2.2

Step 4  Configure dynamic NAT for the object IP addresses. You can only define a single NAT rule for a given object.

nat [(real_ifc,mapped_ifc)] dynamic mapped_obj [interface [ipv6]] [dns]

Where:

• Interfaces—(Required for bridge group member interfaces.) Specify the real (real_ifc) and mapped (mapped_ifc) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the
real and mapped interfaces, all interfaces are used. You can also specify the keyword any for one or both of the interfaces, for example (any,outside), but any does not apply to bridge group member interfaces.

- Mapped IP address—Specify the network object or network object group that includes the mapped IP addresses.

- Interface PAT fallback—(Optional) The interface keyword enables interface PAT fallback. After the mapped IP addresses are used up, then the IP address of the mapped interface is used. If you specify ipv6, then the IPv6 address of the interface is used. For this option, you must configure a specific interface for the mapped_ifc. (You cannot specify interface when the mapped interface is a bridge group member.)

- DNS—(Optional) The dns keyword translates DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See Rewriting DNS Queries and Responses Using NAT, on page 274 for more information.

Example:

```plaintext
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

Examples

The following example configures dynamic NAT that hides the 192.168.2.0 network behind a range of outside addresses 10.2.2.1 through 10.2.2.10:

```plaintext
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

The following example configures dynamic NAT with dynamic PAT backup. Hosts on inside network 10.76.11.0 are mapped first to the nat-range1 pool (10.10.10.10-10.10.10.20). After all addresses in the nat-range1 pool are allocated, dynamic PAT is performed using the pat-ip1 address (10.10.10.21). In the unlikely event that the PAT translations are also used up, dynamic PAT is performed using the outside interface address.

```plaintext
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20
hostname(config)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21
hostname(config)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1
hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

The following example configures dynamic NAT with dynamic PAT backup to translate IPv6 hosts to IPv4. Hosts on inside network 2001:DB8::/96 are mapped first to the IPv4_NAT_RANGE pool.
Configure Dynamic Twice NAT

This section describes how to configure twice NAT for dynamic NAT.

Procedure

Step 1
Create host or range network objects (object network command), or network object groups (object-group network command), for the source real addresses, the source mapped addresses, the destination real addresses, and the destination mapped addresses.

- If you want to translate all source traffic, you can skip adding an object for the source real addresses, and instead specify the any keyword in the nat command.

- If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses, and instead specify the interface keyword in the nat command.

If you do create objects, consider the following guidelines:

- You typically configure a larger group of real addresses to be mapped to a smaller group.

- The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.

- If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.

Step 2
(Optional.) Create service objects for the destination real ports and the destination mapped ports.

For dynamic NAT, you can only perform port translation on the destination. A service object can contain both a source and destination port, but only the destination port is used in this case. If you specify the source port, it will be ignored.

Step 3
Configure dynamic NAT.
Configure Dynamic Twice NAT

nat \( ([\text{real}_\text{ifc},\text{mapped}_\text{ifc}] [\text{line} | \{\text{after-auto} [\text{line}]\}]) \) source dynamic \{\text{real}_\text{obj} | \text{any}\} \{\text{mapped}_\text{obj} [\text{interface} [\text{ipv6}] | [\text{destination} \text{static} \{\text{mapped}_\text{obj} | \text{interface} [\text{ipv6}] \} \text{real}_\text{obj}] \{\text{service} \text{mapped}_\text{dest}_\text{svc}_\text{obj} \text{real}_\text{dest}_\text{svc}_\text{obj}] [\text{dns}] [\text{unidirectional}] [\text{inactive}] [\text{description} \text{desc}] \)

Where:

- **Interfaces**—(Required for bridge group member interfaces.) Specify the real \( \text{real}_\text{ifc} \) and mapped \( \text{mapped}_\text{ifc} \) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword \text{any} for one or both of the interfaces, for example (any,outside), but \text{any} does not apply to bridge group member interfaces.

- **Section and Line**—(Optional.) By default, the NAT rule is added to the end of section 1 of the NAT table (see \text{NAT Rule Order}, on page 204). If you want to add the rule into section 3 instead (after the network object NAT rules), then use the \text{after-auto} keyword. You can insert a rule anywhere in the applicable section using the \text{line} argument.

- **Source addresses**:
  - Real—Specify a network object, group, or the \text{any} keyword.
  - Mapped—Specify a different network object or group. You can optionally configure the following fallback method:
    - Interface PAT fallback—(Optional.) The \text{interface} keyword enables interface PAT fallback. After the mapped IP addresses are used up, then the IP address of the mapped interface is used. If you specify \text{ipv6}, then the IPv6 address of the interface is used. For this option, you must configure a specific interface for the \text{mapped}_\text{ifc}. (You cannot specify \text{interface} when the mapped interface is a bridge group member).

- **Destination addresses** (Optional):
  - Mapped—Specify a network object or group, or for static interface NAT with port translation only, specify the \text{interface} keyword. If you specify \text{ipv6}, then the IPv6 address of the interface is used. If you specify \text{interface}, be sure to also configure the \text{service} keyword. For this option, you must configure a specific interface for the \text{real}_\text{ifc}. See \text{Static NAT with Port Translation}, on page 230 for more information.
  - Real—Specify a network object or group. For identity NAT, simply use the same object or group for both the real and mapped addresses.

- **Destination port**—(Optional.) Specify the \text{service} keyword along with the mapped and real service objects. For identity port translation, simply use the same service object for both the real and mapped ports.

- **DNS**—(Optional; for a source-only rule.) The \text{dns} keyword translates DNS replies. Be sure DNS inspection is enabled (it is enabled by default). You cannot configure the \text{dns} keyword if you configure a \text{destination} address. See \text{Rewriting DNS Queries and Responses Using NAT}, on page 274 for more information.

- **Unidirectional**—(Optional.) Specify \text{unidirectional} so the destination addresses cannot initiate traffic to the source addresses.

- **Inactive**—(Optional.) To make this rule inactive without having to remove the command, use the \text{inactive} keyword. To reactivate it, reenter the whole command without the \text{inactive} keyword.

- **Description**—(Optional.) Provide a description up to 200 characters using the \text{description} keyword.
Configure Dynamic Twice NAT

Example:

hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC

Examples

The following example configures dynamic NAT for inside network 10.1.1.0/24 when accessing servers on the 209.165.201.1/27 network as well as servers on the 203.0.113.0/24 network:

hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2

The following example configures dynamic NAT for an IPv6 inside network 2001:DB8:AAAA::/96 when accessing servers on the IPv4 209.165.201.1/27 network as well as servers on the 203.0.113.0/24 network:

hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10

218
Dynamic PAT

The following topics describe dynamic PAT.

About Dynamic PAT

Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port. If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. If you have a lot of traffic that uses the lower port ranges, you can specify a flat range of ports to be used instead of the three unequal-sized tiers.

Each connection requires a separate translation session because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The following figure shows a typical dynamic PAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back. The mapped address is the same for each translation, but the port is dynamically assigned.

*Figure 20: Dynamic PAT*

For the duration of the translation, a remote host on the destination network can initiate a connection to the translated host if an access rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

After the connection expires, the port translation also expires. For multi-session PAT, the PAT timeout is used, 30 seconds by default. For per-session PAT, the xlate is immediately removed.

*Note*

We recommend that you use different PAT pools for each interface. If you use the same pool for multiple interfaces, especially if you use it for "any" interface, the pool can be quickly exhausted, with no ports available for new translations.

Dynamic PAT Disadvantages and Advantages

Dynamic PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the ASA interface IP address as the PAT address.
You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.

Dynamic PAT does not work with some multimedia applications that have a data stream that is different from the control path. See Default Inspections and NAT Limitations, on page 311 for more information about NAT and PAT support.

Dynamic PAT might also create a large number of connections appearing to come from a single IP address, and servers might interpret the traffic as a DoS attack. You can configure a PAT pool of addresses and use a round-robin assignment of PAT addresses to mitigate this situation.

**PAT Pool Object Guidelines**

When creating network objects for a PAT pool, follow these guidelines.

**For a PAT pool**

- If available, the real source port number is used for the mapped port. However, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. If you have a lot of traffic that uses the lower port ranges, you can specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.

- If you enable block allocation for a PAT pool, port blocks are allocated in the 1024-65535 range only. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host.

- If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT and a flat range, then the other rule must also specify extended PAT and a flat range.

**For extended PAT for a PAT pool**

- Many application inspections do not support extended PAT. See Default Inspections and NAT Limitations, on page 311 for a complete list of unsupported inspections.

- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT with port translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.

- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.

- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.

**For round robin for a PAT pool**

- If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. However, this “stickiness” does not survive a failover. If the device fails over, then subsequent connections from a host might not use the initial IP address.
• IP address “stickiness” is also impacted if you mix PAT pool/round robin rules with interface PAT rules on the same interface. For any given interface, choose either a PAT pool or interface PAT; do not create competing PAT rules.

• Round robin, especially when combined with extended PAT, can consume a large amount of memory. Because NAT pools are created for every mapped protocol/IP address/port range, round robin results in a large number of concurrent NAT pools, which use memory. Extended PAT results in an even larger number of concurrent NAT pools.

Configure Dynamic Network Object PAT

This section describes how to configure network object NAT for dynamic PAT.

Procedure

Step 1  (Optional.) Create a host or range network object (object network command), or a network object group (object-group network command), for the mapped addresses.

• Instead of using an object, you can optionally configure an inline host address or specify the interface address.

• If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.

Step 2  Create or edit the network object for which you want to configure NAT: object network obj_name

Example:

hostname(config)# object network my-host-obj1

Step 3  (Skip when editing an object that has the right address.) Define the real IPv4 or IPv6 addresses that you want to translate.

• host {IPv4_address |IPv6_address}—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.

• subnet {IPv4_address IPv4_mask | IPv6_address /IPv6_prefix}—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

• range start_address end_address—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

Example:

hostname(config-network-object)# range 10.1.1.1 10.1.1.90

Step 4  Configure dynamic PAT for the object IP addresses. You can only define a single NAT rule for a given object.
nat \((\text{real}_\text{ifc},\text{mapped}_\text{ifc})\) \text{dynamic} \((\text{mapped}_\text{inline}_\text{host}_\text{ip} | \text{mapped}_\text{obj} | \text{pat-pool} \text{ mapped}_\text{obj} | \text{round-robin} | \text{extended} | \text{flat [include-reserve]} | \text{block-allocation} | \text{interface [ipv6]} ) | \text{interface [ipv6]} \]

Where:

- **Interfaces**—(Required for bridge group member interfaces.) Specify the real (\text{real}_\text{ifc}) and mapped (\text{mapped}_\text{ifc}) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword \text{any} for one or both of the interfaces, for example (\text{any,outside}), but \text{any} does not apply to bridge group member interfaces.

- **Mapped IP address**—You can specify the mapped IP address as:
  - \text{mapped}_\text{inline}_\text{host}_\text{ip}—An inline host address.
  - \text{mapped}_\text{obj}—A network object that is defined as a host address.
  - \text{pat-pool} \text{ mapped}_\text{obj}—A network object or group that contains multiple addresses.

- **interface [ipv6]**—The IP address of the mapped interface is used as the mapped address. If you specify \text{ipv6}, then the IPv6 address of the interface is used. For this option, you must configure a specific interface for the \text{mapped}_\text{ifc}. (You cannot specify \text{interface} when the mapped interface is a bridge group member.) You must use this keyword when you want to use the interface IP address; you cannot enter it inline or as an object.

- **For a PAT pool, you can specify one or more of the following options:**
  - \text{round-robin}—Enables round-robin address allocation for a PAT pool. Without round robin, by default all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns an address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
  - \text{extended}—Enables extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.
  - \text{flat [include-reserve]}—(Flat range) Enables use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also specify the \text{include-reserve} keyword.
  - \text{block-allocation}—Enables port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with \text{round-robin}, but you cannot use the \text{extended} or \text{flat [include-reserve]} options. You also cannot use interface PAT fallback.

- **Interface PAT fallback**—(Optional.) The \text{interface [ipv6]} keyword enables interface PAT fallback when entered after a primary PAT address. After the primary PAT addresses are used up, then the IP address of the mapped interface is used. If you specify \text{ipv6}, then the IPv6 address of the interface is used. For
this option, you must configure a specific interface for the \textit{mapped_ifc}. (You cannot specify \textit{interface} when the mapped interface is a bridge group member.)

\textbf{Example:}

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

\textbf{Examples}

The following example configures dynamic PAT that hides the 192.168.2.0 network behind address 10.2.2.2:

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

The following example configures dynamic PAT that hides the 192.168.2.0 network behind the outside interface address:

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

The following example configures dynamic PAT with a PAT pool to translate the inside IPv6 network to an outside IPv4 network:

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

\section*{Configure Dynamic Twice PAT}

This section describes how to configure twice NAT for dynamic PAT.

\textbf{Procedure}

\textbf{Step 1} Create host or range network objects (\texttt{object network} command), or network object groups (\texttt{object-group network} command), for the source real addresses, the source mapped addresses, the destination real addresses, and the destination mapped addresses.

- If you want to translate all source traffic, you can skip adding an object for the source real addresses, and instead specify the \texttt{any} keyword in the \texttt{nat} command.

- If you want to use the interface address as the mapped address, you can skip adding an object for the source mapped addresses, and instead specify the \texttt{interface} keyword in the \texttt{nat} command.
• If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses, and instead specify the `interface` keyword in the `nat` command.

If you use an object, the object or group cannot contain a subnet. The object must define a host, or for a PAT pool, a range. The group (for a PAT pool) can include hosts and ranges.

**Step 2** (Optional.) Create service objects for the destination real ports and the destination mapped ports.

For dynamic NAT, you can only perform port translation on the destination. A service object can contain both a source and destination port, but only the destination port is used in this case. If you specify the source port, it will be ignored.

**Step 3** Configure dynamic PAT.

```
nat [(real_ifc,mapped_ifc)] [line | after-auto [line]] source dynamic {real-obj | any} {mapped_obj [interface [ipv6]] | pat-pool mapped-obj [round-robin] [extended] [flat [include-reserve]] [block-allocation] [interface [ipv6]] [interface [ipv6]] [destination static {mapped_obj | interface [ipv6]}] real_obj [service mapped_dest_svc_obj real_dest_svc_obj] [unidirectional] [inactive] [description description]
```

Where:

• Interfaces—(Required for bridge group member interfaces.) Specify the real (`real_ifc`) and mapped (`mapped_ifc`) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword `any` for one or both of the interfaces, for example (any,outside), but `any` does not apply to bridge group member interfaces.

• Section and Line—(Optional.) By default, the NAT rule is added to the end of section 1 of the NAT table (see NAT Rule Order, on page 204). If you want to add the rule into section 3 instead (after the network object NAT rules), then use the `after-auto` keyword. You can insert a rule anywhere in the applicable section using the `line` argument.

• Source addresses:

  • Real—A network object, group, or the `any` keyword. Use the `any` keyword if you want to translate all traffic from the real interface to the mapped interface.

  • Mapped—Configure one of the following:

    • Network object—A network object that contains a host address.

    • `pat-pool mapped-obj`—A network object or group that contains multiple addresses.

    • `interface [ipv6]`—(Routed mode only.) The IP address of the mapped interface is used as the mapped address (interface PAT). If you specify `ipv6`, then the IPv6 address of the interface is used. For this option, you must configure a specific interface for the `mapped_ifc`. (You cannot specify `interface` when the mapped interface is a bridge group member.) If you specify this keyword with a PAT pool or network object, you are enabling interface PAT fallback. After the PAT IP addresses are used up, then the IP address of the mapped interface is used.

For a PAT pool, you can specify one or more of the following options:

  • `round-robin`—Enables round-robin address allocation for a PAT pool. Without round robin, by default all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns an address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
• **extended**—Enables extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

• **flat [include-reserve]**—(Flat range) Enables use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also specify the include-reserve keyword.

• **block-allocation**—Enables port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with **round-robin**, but you cannot use the extended or flat [include-reserve] options. You also cannot use interface PAT fallback.

• Destination addresses (Optional):
  - Mapped—Specify a network object or group, or for static interface NAT with port translation only (non-bridge group member interfaces only), specify the interface keyword. If you specify ipv6, then the IPv6 address of the interface is used. If you specify interface, be sure to also configure the service keyword. For this option, you must configure a specific interface for the real_ifc. See Static NAT with Port Translation, on page 230 for more information.
  - Real—Specify a network object or group. For identity NAT, simply use the same object or group for both the real and mapped addresses.

• Destination port—(Optional.) Specify the service keyword along with the mapped and real service objects. For identity port translation, simply use the same service object for both the real and mapped ports.

• Unidirectional—(Optional.) Specify unidirectional so the destination addresses cannot initiate traffic to the source addresses.

• Inactive—(Optional.) To make this rule inactive without having to remove the command, use the inactive keyword. To reactivate it, reenter the whole command without the inactive keyword.

• Description—(Optional.) Provide a description up to 200 characters using the description keyword.

**Example:**

hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
description Interface PAT for inside addresses when going to server 1
Configure PAT with Port Block Allocation

For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated.
if the host has active connections for all ports in the original block. Blocks are freed when the last xlate that uses a port in the block is removed.

The main reason for allocating port blocks is reduced logging. The port block allocation is logged, connections are logged, but xlates created within the port block are not logged. On the other hand, this makes log analysis more difficult.

Port blocks are allocated in the 1024-65535 range only. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host. You can create a separate NAT rule that does not use block allocation for applications that use low port numbers; for twice NAT, ensure the rule comes before the block allocation rule.

**Before you begin**

Usage notes for NAT rules:

- You can include the `round-robin` keyword, but you cannot include `extended`, `flat`, `include-reserve`, or `interface` (for interface PAT fallback). Other source/destination address and port information is also allowed.

- As with all NAT changes, if you replace an existing rule, you must clear xlates related to the replaced rule to have the new rule take effect. You can clear them explicitly or simply wait for them to time out.

- For a given PAT pool, you must specify (or not specify) block allocation for all rules that use the pool. You cannot allocate blocks in one rule and not in another. PAT pools that overlap also cannot mix block allocation settings. You also cannot overlap static NAT with port translation rules with the pool.

**Procedure**

**Step 1**  
(Optional.) Configure the block allocation size, which is the number of ports in each block.

```plaintext
xlate block-allocation size value
```

The range is 32-4096. The default is 512. Use the “no” form to return to the default.

If you do not use the default, ensure that the size you choose divides evenly into 64,512 (the number of ports in the 1024-65535 range). Otherwise, there will be ports that cannot be used. For example, if you specify 100, there will be 12 unused ports.

**Step 2**  
(Optional.) Configure the maximum blocks that can be allocated per host.

```plaintext
xlate block-allocation maximum-per-host number
```

The limit is per protocol, so a limit of 4 means at most 4 UDP blocks, 4 TCP blocks, and 4 ICMP blocks per host. The range is 1-8, the default is 4. Use the “no” form to return to the default.

**Step 3**  
Add NAT rules that use PAT pool block allocation.

- **Object PAT.**

  ```plaintext
  nat [(real_ifc,mapped_ifc)] dynamic pat-pool mapped-obj block-allocation
  ```

  Example:

  ```plaintext
  object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
  ```
Configure Per-Session PAT or Multi-Session PAT

By default, all TCP PAT traffic and all UDP DNS traffic uses per-session PAT. To use multi-session PAT for traffic, you can configure per-session PAT rules: a permit rule uses per-session PAT, and a deny rule uses multi-session PAT.

Per-session PAT improves the scalability of PAT and, for clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds.

For “hit-and-run” traffic, such as HTTP or HTTPS, per-session PAT can dramatically increase the connection rate supported by one address. Without per-session PAT, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With per-session PAT, the connection rate for one address for an IP protocol is 65535/average-lifetime.

For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule. However, if you also want to use per-session PAT for the UDP ports used by these protocols, you must create the permit rules for them.

Before you begin

By default, the following rules are installed:

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
```
You cannot remove these rules, and they always exist after any manually-created rules. Because rules are evaluated in order, you can override the default rules. For example, to completely negate these rules, you could add the following:

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

**Procedure**

Create a permit or deny per-session PAT rule. This rule is placed above the default rules, but below any other manually-created rules. Be sure to create your rules in the order you want them applied.

```
xlate per-session {permit | deny} {tcp | udp} source_ip [operator src_port] destination_ip [operator dest_port]
```

For the source and destination IP addresses, you can configure the following:

- **host ip_address**—Specifies an IPv4 or IPv6 host address.
- **ip_address mask**—Specifies an IPv4 network address and subnet mask.
- **ipv6-address/prefix-length**—Specifies an IPv6 network address and prefix.
- **any4 and any6**—any4 specifies only IPv4 traffic; and any6 specifies any6 traffic.

The **operator** matches the port numbers used by the source or destination. The default is all ports. The permitted operators are:

- **lt**—less than
- **gt**—greater than
- **eq**—equal to
- **neq**—not equal to
- **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example, range 100 200.

**Example**

The following example creates a deny rule for H.323 traffic, so that it uses multi-session PAT:

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
```
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719

The following example enables the distribution of SIP across the members of a cluster by permitting per-session PAT for the SIP UDP port. Per-session PAT is the default for SIP TCP ports, so you do not need a rule for TCP unless you altered the default rules.

hostname(config)# xlate per-session permit udp any4 any4 eq sip

**Static NAT**

The following topics explain static NAT and how to implement it.

### About Static NAT

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an access rule exists that allows it). With dynamic NAT and PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

The following figure shows a typical static NAT scenario. The translation is always active so both real and remote hosts can initiate connections.

**Figure 21: Static NAT**

You can disable bidirectionality if desired.

### Static NAT with Port Translation

Static NAT with port translation lets you specify a real and mapped protocol and port.

When you specify the port with static NAT, you can choose to map the port and/or the IP address to the same value or to a different value.

The following figure shows a typical static NAT with port translation scenario showing both a port that is mapped to itself and a port that is mapped to a different value; the IP address is mapped to a different value in both cases. The translation is always active so both translated and remote hosts can initiate connections.
Static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. In addition, for twice NAT, traffic that does not match the source IP address of the NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, you must add additional rules for all other traffic allowed to the destination IP address. For example, you can configure a static NAT rule for the IP address, without port specification, and place it after the port translation rule.

**Note**

For applications that require application inspection for secondary channels (for example, FTP and VoIP), NAT automatically translates the secondary ports.

Following are some other uses of static NAT with port translation.

**Static NAT with Identity Port Translation**

You can simplify external access to internal resources. For example, if you have three separate servers that provide services on different ports (such as FTP, HTTP, and SMTP), you can give external users a single IP address to access those services. You can then configure static NAT with identity port translation to map the single external IP address to the correct IP addresses of the real servers based on the port they are trying to access. You do not need to change the port, because the servers are using the standard ones (21, 80, and 25 respectively). For details on how to configure this example, see Single Address for FTP, HTTP, and SMTP (Static NAT-with-Port-Translation), on page 253.

**Static NAT with Port Translation for Non-Standard Ports**

You can also use static NAT with port translation to translate a well-known port to a non-standard port or vice versa. For example, if inside web servers use port 8080, you can allow outside users to connect to port 80, and then undo translation to the original port 8080. Similarly, to provide extra security, you can tell web users to connect to non-standard port 6785, and then undo translation to port 80.

**Static Interface NAT with Port Translation**

You can configure static NAT to map a real address to an interface address/port combination. For example, if you want to redirect Telnet access for the device's outside interface to an inside host, then you can map the inside host IP address/port 23 to the outside interface address/port 23.

**One-to-Many Static NAT**

Typically, you configure static NAT with a one-to-one mapping. However, in some cases, you might want to configure a single real address to several mapped addresses (one-to-many). When you configure one-to-many static NAT, when the real host initiates traffic, it always uses the first mapped address. However, for traffic initiated to the host, you can initiate traffic to any of the mapped addresses, and they will be untranslated to the single real address.
The following figure shows a typical one-to-many static NAT scenario. Because initiation by the real host always uses the first mapped address, the translation of real host IP/first mapped IP is technically the only bidirectional translation.

**Figure 23: One-to-Many Static NAT**

For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server. For details on how to configure this example, see *Inside Load Balancer with Multiple Mapped Addresses (Static NAT, One-to-Many)*, on page 252.

**Figure 24: One-to-Many Static NAT Example**

**Other Mapping Scenarios (Not Recommended)**

NAT has the flexibility to allow any kind of static mapping scenario: one-to-one, one-to-many, but also few-to-many, many-to-few, and many-to-one mappings. We recommend using only one-to-one or one-to-many mappings. These other mapping options might result in unintended consequences.
Functionally, few-to-many is the same as one-to-many; but because the configuration is more complicated and the actual mappings may not be obvious at a glance, we recommend creating a one-to-many configuration for each real address that requires it. For example, for a few-to-many scenario, the few real addresses are mapped to the many mapped addresses in order (A to 1, B to 2, C to 3). When all real addresses are mapped, the next mapped address is mapped to the first real address, and so on until all mapped addresses are mapped (A to 4, B to 5, C to 6). This results in multiple mapped addresses for each real address. Just like a one-to-many configuration, only the first mappings are bidirectional; subsequent mappings allow traffic to be initiated to the real host, but all traffic from the real host uses only the first mapped address for the source.

The following figure shows a typical few-to-many static NAT scenario.

*Figure 25: Few-to-Many Static NAT*

For a many-to-few or many-to-one configuration, where you have more real addresses than mapped addresses, you run out of mapped addresses before you run out of real addresses. Only the mappings between the lowest real IP addresses and the mapped pool result in bidirectional initiation. The remaining higher real addresses can initiate traffic, but traffic cannot be initiated to them (returning traffic for a connection is directed to the correct real address because of the unique 5-tuple (source IP, destination IP, source port, destination port, protocol) for the connection).

**Note**

Many-to-few or many-to-one NAT is not PAT. If two real hosts use the same source port number and go to the same outside server and the same TCP destination port, and both hosts are translated to the same IP address, then both connections will be reset because of an address conflict (the 5-tuple is not unique).

The following figure shows a typical many-to-few static NAT scenario.

*Figure 26: Many-to-Few Static NAT*

Instead of using a static rule this way, we suggest that you create a one-to-one rule for the traffic that needs bidirectional initiation, and then create a dynamic rule for the rest of your addresses.
Configure Static Network Object NAT or Static NAT-with-Port-Translation

This section describes how to configure a static NAT rule using network object NAT.

Procedure

Step 1  (Optional.) Create a network object (object network command), or a network object group (object-group network command), for the mapped addresses.

- Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).
- If you use an object, the object or group can contain a host, range, or subnet.

Step 2  Create or edit the network object for which you want to configure NAT: object network obj_name

Example:

hostname(config)# object network my-host-obj1

Step 3  (Skip when editing an object that has the right address.) Define the real IPv4 or IPv6 addresses that you want to translate.

- host {IPv4_address | IPv6_address}—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.
- subnet {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}—The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.
- range start_address end_address—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

Example:

hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0

Step 4  Configure static NAT for the object IP addresses. You can only define a single NAT rule for a given object.

nat [(real_ifc,mapped_ifc)] static {mapped_inline_host_ip | mapped_obj | interface [ipv6]} [net-to-net] [dns | service {tcp | udp | sctp} real_port mapped_port] [no-proxy-arp]

Where:

- Interfaces—(Required for bridge group member interfaces.) Specify the real (real_ifc) and mapped (mapped_ifc) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword any for one or both of the interfaces, for example (any,outside), but any does not apply to bridge group member interfaces.

- Mapped IP address—You can specify the mapped IP address as one of the following. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses. See Static NAT, on page 230.
Network Address Translation

Configure Static Network Object NAT or Static NAT-with-Port-Translation

- **mapped_inline_host_ip**—An inline host IP address. This provides a one-to-one mapping for host objects only. Otherwise, you get a many-to-one mapping. For NAT46 or NAT66 translations, this can be an IPv6 network address.

- **mapped_obj**—An existing network object or group. To do a one-to-one mapping for a range of IP addresses, select an object that contains a range with the same number of addresses.

- **interface**—(Static NAT-with-port-translation only.) The IP address of the mapped interface is used as the mapped address. If you specify ipv6, then the IPv6 address of the interface is used. For this option, you must configure a specific interface for the mapped_ifc. (You cannot specify interface when the mapped interface is a bridge group member.) You must use this keyword when you want to use the interface IP address; you cannot enter it inline or as an object. Be sure to also configure the service keyword.

- Net-to-net—(Optional.) For NAT 46, specify net-to-net to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this keyword.

- DNS—(Optional.) The dns keyword translates DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See Rewriting DNS Queries and Responses Using NAT, on page 274 for more information.

- Port translation—(Static NAT-with-port-translation only.) Specify service with the desired protocol keyword and the real and mapped ports. You can enter either a port number or a well-known port name (such as http).

- No Proxy ARP—(Optional.) Specify no-proxy-arp to disable proxy ARP for incoming packets to the mapped IP addresses. For information on the conditions which might require the disabling of proxy ARP, see Mapped Addresses and Routing, on page 261.

**Example:**

hostname(config-network-object)#
nat (inside,outside) static MAPPED_IPS service tcp 80 8080

---

**Examples**

The following example configures static NAT for the real host 10.1.1.1 on the inside to 10.2.2.2 on the outside with DNS rewrite enabled.

hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns

The following example configures static NAT for the real host 10.1.1.1 on the inside to 10.2.2.2 on the outside using a mapped object.

hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2
hostname(config-network-object)# object network my-host-obj1
Configure Static Twice NAT or Static NAT-with-Port-Translation

This section describes how to configure a static NAT rule using twice NAT.

Procedure

Step 1

Create host or range network objects (object network command), or network object groups (object-group network command), for the source real addresses, the source mapped addresses, the destination real addresses, and the destination mapped addresses.

- If you want to configure source static interface NAT with port translation only, you can skip adding an object for the source mapped addresses, and instead specify the interface keyword in the nat command.
- If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses, and instead specify the interface keyword in the nat command.

If you do create objects, consider the following guidelines:

- The mapped object or group can contain a host, range, or subnet.
- The static mapping is typically one-to-one, so the real addresses have the same quantity as the mapped addresses. You can, however, have different quantities if desired. For more information, see Static NAT, on page 230.

Step 2

(Optional.) Create service objects for the:

- Source or Destination real ports
• Source or Destination mapped ports

A service object can contain both a source and destination port; however, you should specify either the source or the destination port for both service objects. You should only specify both the source and destination ports if your application uses a fixed source port (such as some DNS servers); but fixed source ports are rare. For example, if you want to translate the port for the source host, then configure the source service.

**Step 3**

Configure **static NAT**.

```
nat [(real_ifc, mapped_ifc)] [line] {after-object [line]}] source static real_ob [mapped_obj | interface [ipv6]] [destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [net-to-net] [dns] [unidirectional | no-proxy-arp] [inactive] [description desc]
```

Where:

- **Interfaces**—(Required for bridge group member interfaces.) Specify the real (real_ifc) and mapped (mapped_ifc) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword any for one or both of the interfaces, for example (any, outside), but any does not apply to bridge group member interfaces.

- **Section and Line**—(Optional.) By default, the NAT rule is added to the end of section 1 of the NAT table (see NAT Rule Order, on page 204). If you want to add the rule into section 3 instead (after the network object NAT rules), then use the after-auto keyword. You can insert a rule anywhere in the applicable section using the line argument.

- **Source addresses:**
  - **Real**—Specify a network object or group. Do not use the any keyword, which would be used for identity NAT.
  - **Mapped**—Specify a different network object or group. For static interface NAT with port translation only, you can specify the interface keyword. If you specify ipv6, then the IPv6 address of the interface is used. If you specify interface, be sure to also configure the service keyword (in this case, the service objects should include only the source port). For this option, you must configure a specific interface for the mapped_ifc. (You cannot specify interface when the mapped interface is a bridge group member.) See Static NAT with Port Translation, on page 230 for more information.

- **Destination addresses** (Optional):
  - **Mapped**—Specify a network object or group, or for static interface NAT with port translation only, specify the interface keyword. If you specify ipv6, then the IPv6 address of the interface is used. If you specify interface, be sure to also configure the service keyword (in this case, the service objects should include only the destination port). For this option, you must configure a specific interface for the real_ifc. (You cannot specify interface when the mapped interface is a bridge group member.)
  - **Real**—Specify a network object or group. For identity NAT, simply use the same object or group for both the real and mapped addresses.

- **Ports**—(Optional.) Specify the service keyword along with the real and mapped service objects. For source port translation, the objects must specify the source service. The order of the service objects in the command for source port translation is service real_obj mapped_obj. For destination port translation, the objects must specify the destination service. The order of the service objects for destination port translation is service mapped_obj real_obj. In the rare case where you specify both the source and
destination ports in the object, the first service object contains the real source port/mapped destination port; the second service object contains the mapped source port/real destination port. For identity port translation, simply use the same service object for both the real and mapped ports (source and/or destination ports, depending on your configuration).

- Net-to-net—(Optional.) For NAT 46, specify **net-to-net** to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this keyword.

- DNS—(Optional; for a source-only rule.) The **dns** keyword translates DNS replies. Be sure DNS inspection is enabled (it is enabled by default). You cannot configure the **dns** keyword if you configure a **destination** address. See Rewriting DNS Queries and Responses Using NAT, on page 274 for more information.

- Unidirectional—(Optional.) Specify **unidirectional** so the destination addresses cannot initiate traffic to the source addresses.

- No Proxy ARP—(Optional.) Specify **no-proxy-arp** to disable proxy ARP for incoming packets to the mapped IP addresses. See Mapped Addresses and Routing, on page 261 for more information.

- Inactive—(Optional.) To make this rule inactive without having to remove the command, use the **inactive** keyword. To reactivate it, reenter the whole command without the **inactive** keyword.

- Description—(Optional.) Provide a description up to 200 characters using the **description** keyword.

**Example:**

```plaintext
hostname(config)# nat (inside, dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

**Examples**

The following example shows the use of static interface NAT with port translation. Hosts on the outside access an FTP server on the inside by connecting to the outside interface IP address with destination port 65000 through 65004. The traffic is untranslated to the internal FTP server at 192.168.10.100:6500 through 65004. Note that you specify the source port range in the service object (and not the destination port) because you want to translate the source address and port as identified in the command; the destination port is “any.” Because static NAT is bidirectional, “source” and “destination” refers primarily to the command keywords; the actual source and destination address and port in a packet depends on which host sent the packet. In this example, connections are originated from outside to inside, so the “source” address and port of the FTP server is actually the destination address and port in the originating packet.

```plaintext
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside, outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

**CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10**

238
The following examples show a static translation of one IPv6 network to another IPv6 when accessing an IPv6 network, and the dynamic PAT translation to an IPv4 PAT pool when accessing the IPv4 network:

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

### Identity NAT

You might have a NAT configuration in which you need to translate an IP address to itself. For example, if you create a broad rule that applies NAT to every network, but want to exclude one network from NAT, you can create a static NAT rule to translate an address to itself. Identity NAT is necessary for remote access VPN, where you need to exempt the client traffic from NAT.

The following figure shows a typical identity NAT scenario.

*Figure 27: Identity NAT*

```
Security
Appliance

209.165.201.1 209.165.201.2

Inside / Outside

209.165.201.1 209.165.201.2
```

The following topics explain how to configure identity NAT.

### Configure Identity Network Object NAT

This section describes how to configure an identity NAT rule using network object NAT.
Procedure

Step 1 (Optional.) Create a network object (object network command), or a network object group (object-group network command), for the mapped addresses.

- Instead of using an object, you can configure an inline address.
- If you use an object, the object must match the real addresses you want to translate.

Step 2 Create or edit the network object for which you want to configure NAT: object network obj_name

The object must be a different one than what you use for the mapped addresses, even though the contents must be the same in each object.

Example:

```
hostname(config)# object network my-host-obj1
```

Step 3 (Skip when editing an object that has the right address.) Define the real IPv4 or IPv6 addresses that you want to translate.

- host {IPv4_address | IPv6_address} — The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.

- subnet {IPv4_address IPv4_mask | IPv6_address IPv6_prefix} — The address of a network. For IPv4 subnets, include the mask after a space, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix as a single unit (no spaces), such as 2001:DB8:0:CD30::/60.

- range start_address end_address — A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.

Example:

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

Step 4 Configure identity NAT for the object IP addresses. You can only define a single NAT rule for a given object.

```
nat ([real_ifc,mapped_ifc]) static {mapped_inline_host_ip | mapped_obj} [no-proxy-arp] [route-lookup]
```

Where:

- Interfaces—(Required for bridge group member interfaces.) Specify the real (real_ifc) and mapped (mapped_ifc) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword any for one or both of the interfaces, for example (any,outside), but any does not apply to bridge group member interfaces.

- Mapped IP addresses—Be sure to configure the same IP address for both the mapped and real address. Use one of the following:
  - mapped_inline_host_ip—An inline host IP address. This provides identity NAT for a host object only.
  - mapped_obj—A network object or group that includes the same addresses as the real object.
• No Proxy ARP—(Optional.) Specify `no-proxy-arp` to disable proxy ARP for incoming packets to the mapped IP addresses. For information on the conditions which might require the disabling of proxy ARP, see Mapped Addresses and Routing, on page 261.

• Route lookup—(Routed mode only; interfaces specified.) Specify `route-lookup` to determine the egress interface using a route lookup instead of using the interface specified in the NAT command. See Determining the Egress Interface, on page 263 for more information.

Example:

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

Example
The following example maps a host address to itself using an inline mapped address:

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

The following example maps a host address to itself using a network object:

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

## Configure Identity Twice NAT

This section describes how to configure an identity NAT rule using twice NAT.

### Procedure

**Step 1**

Create host or range network objects (`object network` command), or network object groups (`object-group network` command), for the source real addresses (you will typically use the same object for the source mapped addresses), the destination real addresses, and the destination mapped addresses.

- If you want to perform identity NAT for all addresses, you can skip creating an object for the source real addresses and instead use the keywords `any any` in the `nat` command.

- If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses, and instead specify the `interface` keyword in the `nat` command.

If you do create objects, consider the following guidelines:
The mapped object or group can contain a host, range, or subnet.

The real and mapped source objects must match. You can use the same object for both, or you can create separate objects that contain the same IP addresses.

**Step 2** (Optional.) Create service objects for the:

- **Source or Destination real ports**
- **Source or Destination mapped ports**

A service object can contain both a source and destination port; however, you should specify either the source or the destination port for both service objects. You should only specify both the source and destination ports if your application uses a fixed source port (such as some DNS servers); but fixed source ports are rare. For example, if you want to translate the port for the source host, then configure the source service.

**Step 3** Configure identity NAT.

```
nat [(real_ifc,mapped_ifc)] [line | {after-object | line}] source static {nw_obj nw_obj | any any} [destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [no-proxy-arp] [route-lookup] [inactive] [description desc]
```

Where:

- **Interfaces**—(Required for bridge group member interfaces.) Specify the real (real_ifc) and mapped (mapped_ifc) interfaces. Be sure to include the parentheses. In routed mode, if you do not specify the real and mapped interfaces, all interfaces are used. You can also specify the keyword any for one or both of the interfaces, for example (any, outside), but any does not apply to bridge group member interfaces.

- **Section and Line**—(Optional.) By default, the NAT rule is added to the end of section 1 of the NAT table (see NAT Rule Order, on page 204). If you want to add the rule into section 3 instead (after the network object NAT rules), then use the after-auto keyword. You can insert a rule anywhere in the applicable section using the line argument.

- **Source addresses**—Specify a network object, group, or the any keyword for both the real and mapped addresses.

- **Destination addresses** (Optional):
  - **Mapped**—Specify a network object or group, or for static interface NAT with port translation only, specify the interface keyword. If you specify ipv6, then the IPv6 address of the interface is used. If you specify interface, be sure to also configure the service keyword (in this case, the service objects should include only the destination port). For this option, you must configure a specific interface for the real_ifc. (You cannot specify interface when the real interface is a bridge group member).
  - **Real**—Specify a network object or group. For identity NAT, simply use the same object or group for both the real and mapped addresses.

- **Ports**—(Optional.) Specify the service keyword along with the real and mapped service objects. For source port translation, the objects must specify the source service. The order of the service objects in the command for source port translation is service real_obj mapped_obj. For destination port translation, the objects must specify the destination service. The order of the service objects for destination port translation is service mapped_obj real_obj. In the rare case where you specify both the source and destination ports in the object, the first service object contains the real source port/mapped destination port; the second service object contains the mapped source port/real destination port. For identity port
translation, simply use the same service object for both the real and mapped ports (source and/or destination ports, depending on your configuration).

- No Proxy ARP—(Optional.) Specify `no-proxy-arp` to disable proxy ARP for incoming packets to the mapped IP addresses. See Mapped Addresses and Routing, on page 261 for more information.

- Route lookup—(Optional; routed mode only; interfaces specified.) Specify `route-lookup` to determine the egress interface using a route lookup instead of using the interface specified in the NAT command. See Determining the Egress Interface, on page 263 for more information.

- Inactive—(Optional.) To make this rule inactive without having to remove the command, use the inactive keyword. To reactivate it, reenter the whole command without the inactive keyword.

- Description—Optional.) Provide a description up to 200 characters using the description keyword.

Example:

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
destination static Server1 Server1
```

---

## Monitoring NAT

To monitor NAT, use the following commands:

- **show nat**
  Shows NAT statistics, including hits for each NAT rule.

- **show nat pool**
  Shows NAT pool statistics, including the addresses and ports allocated, and how many times they were allocated.

- **show running-config nat**
  Shows the NAT configuration. You cannot see object NAT rules using `show running-config object`. When you use show running-config without modifiers, objects that include NAT rules are shown twice, first with the basic address configuration, then later in the configuration, the object with the NAT rule. The complete object, with the address and NAT rule, is not shown as a unit.

- **show xlate**
  Shows current NAT session information.
# History for NAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Object NAT | 8.3(1) | Configures NAT for a network object IP address(es).
We introduced or modified the following commands: **nat** (object network configuration mode), **show nat, show xlate, show nat pool**. |
| Twice NAT | 8.3(1) | Twice NAT lets you identify both the source and destination address in a single rule.
We modified or introduced the following commands: **nat, show nat, show xlate, show nat pool**. |
| Identity NAT configurable proxy ARP and route lookup | 8.4(2)/8.5(1) | In earlier releases for identity NAT, proxy ARP was disabled, and a route lookup was always used to determine the egress interface. You could not configure these settings. In 8.4(2) and later, the default behavior for identity NAT was changed to match the behavior of other static NAT configurations: proxy ARP is enabled, and the NAT configuration determines the egress interface (if specified) by default. You can leave these settings as is, or you can enable or disable them discretely. Note that you can now also disable proxy ARP for regular static NAT. 
For pre-8.3 configurations, the migration of NAT exempt rules (the **nat 0 access-list** command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: **no-proxy-arp** and **route-lookup**. The **unidirectional** keyword that was used for migrating to 8.3(2) and 8.4(1) is no longer used for migration. When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed. 
We modified the following command: **nat static [no-proxy-arp] [route-lookup]**. |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAT pool and round robin address assignment</td>
<td>8.4(2)/8.5(1)</td>
<td>You can now specify a pool of PAT addresses instead of a single address. You can also optionally enable round-robin assignment of PAT addresses instead of first using all ports on a PAT address before using the next address in the pool. These features help prevent a large number of connections from a single PAT address from appearing to be part of a DoS attack and makes configuration of large numbers of PAT addresses easy.</td>
</tr>
<tr>
<td>We modified the following commands: <em>nat dynamic [pat-pool mapped_object [round-robin]]</em> and <em>nat source dynamic [pat-pool mapped_object [round-robin]]</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Round robin PAT pool allocation uses the same IP address for existing hosts</td>
<td>8.4(3)</td>
<td>When using a PAT pool with round robin allocation, if a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. We did not modify any commands. <em>This feature is not available in 8.5(1) or 8.6(1).</em></td>
</tr>
<tr>
<td>Flat range of PAT ports for a PAT pool</td>
<td>8.4(3)</td>
<td>If available, the real source port number is used for the mapped port. However, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool. If you have a lot of traffic that uses the lower port ranges, when using a PAT pool, you can now specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535. We modified the following commands: <em>nat dynamic [pat-pool mapped_object [flat [include-reserve]]]</em> and <em>nat source dynamic [pat-pool mapped_object [flat [include-reserve]]]</em>. <em>This feature is not available in 8.5(1) or 8.6(1).</em></td>
</tr>
<tr>
<td>Extended PAT for a PAT pool</td>
<td>8.4(3)</td>
<td>Each PAT IP address allows up to 65535 ports. If 65535 ports do not provide enough translations, you can now enable extended PAT for a PAT pool. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. We modified the following command: <em>nat dynamic [pat-pool mapped_object [extended]]</em> and *nat source dynamic [pat-pool mapped_object [extended]]. <em>This feature is not available in 8.5(1) or 8.6(1).</em></td>
</tr>
</tbody>
</table>
In rare situations, you might want to use a VPN peer’s real IP address on the inside network instead of an assigned local IP address. Normally with VPN, the peer is given an assigned local IP address to access the inside network. However, you might want to translate the local IP address back to the peer’s real public IP address if, for example, your inside servers and network security is based on the peer’s real IP address.

You can enable this feature on one interface per tunnel group. Object NAT rules are dynamically added and deleted when the VPN session is established or disconnected. You can view the rules using the `show nat` command.

Because of routing issues, we do not recommend using this feature unless you know you need it; contact Cisco TAC to confirm feature compatibility with your network. See the following limitations:

- Only supports Cisco IPsec and AnyConnect Client.
- Return traffic to the public IP addresses must be routed back to the ASA so the NAT policy and VPN policy can be applied.
- Does not support load-balancing (because of routing issues).
- Does not support roaming (public IP changing).

We introduced the following command: `nat-assigned-to-public-ip interface` (tunnel-group general-attributes configuration mode).

### NAT support for IPv6

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0(1)</td>
<td>NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6. Translating between IPv4 and IPv6 is not supported in transparent mode.</td>
<td></td>
</tr>
</tbody>
</table>

We modified the following commands: `nat` (global and object network configuration modes), `show nat`, `show nat pool`, `show xlate`.

### NAT support for reverse DNS lookups

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0(1)</td>
<td>NAT now supports translation of the DNS PTR record for reverse DNS lookups when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection enabled for the NAT rule.</td>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Per-session PAT</td>
<td>9.0(1)</td>
<td>The per-session PAT feature improves the scalability of PAT and, for clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For “hit-and-run” traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is ( \frac{65535}{\text{average-lifetime}} ). By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that requires multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule. We introduced the following commands: <code>xlate per-session</code>, <code>show nat pool</code>.</td>
</tr>
<tr>
<td>Transactional Commit Model on NAT Rule Engine</td>
<td>9.3(1)</td>
<td>When enabled, a NAT rule update is applied after the rule compilation is completed; without affecting the rule matching performance. We added the <code>nat</code> keyword to the following commands: <code>asp rule-engine transactional-commit</code>, <code>show running-config asp rule-engine transactional-commit</code>, <code>clear configure asp rule-engine transactional-commit</code>. We added NAT to the following screen: Configuration &gt; Device Management &gt; Advanced &gt; Rule Engine.</td>
</tr>
<tr>
<td>Carrier Grade NAT enhancements</td>
<td>9.5(1)</td>
<td>For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). We added the following commands: <code>xlate block-allocation size</code>, <code>xlate block-allocation maximum-per-host</code>. We added the <code>block-allocation</code> keyword to the <code>nat</code> command.</td>
</tr>
<tr>
<td>NAT support for SCTP</td>
<td>9.5(2)</td>
<td>You can now specify SCTP ports in static network object NAT rules. Using SCTP in static twice NAT is not recommended. Dynamic NAT/PAT does not support SCTP. We modified the following commands: <code>nat static</code> (object).</td>
</tr>
</tbody>
</table>
NAT Examples and Reference

The following topics provide examples for configuring NAT, plus information on advanced configuration and troubleshooting.

- Examples for Network Object NAT, on page 249
- Examples for Twice NAT, on page 254
- NAT in Routed and Transparent Mode, on page 258
- Routing NAT Packets, on page 260
- NAT for VPN, on page 263
- Translating IPv6 Networks, on page 269
- Rewriting DNS Queries and Responses Using NAT, on page 274

Examples for Network Object NAT

Following are some configuration examples for network object NAT.

Providing Access to an Inside Web Server (Static NAT)

The following example performs static NAT for an inside web server. The real address is on a private network, so a public address is required. Static NAT is necessary so hosts can initiate traffic to the web server at a fixed address.
Figure 28: Static NAT for an Inside Web Server

```
Step 1
Create a network object for the internal web server.

hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27

Step 2
Configure static NAT for the object:

hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

**NAT for Inside Hosts (Dynamic NAT) and NAT for an Outside Web Server (Static NAT)**

The following example configures dynamic NAT for inside users on a private network when they access the outside. Also, when inside users connect to an outside web server, that web server address is translated to an address that appears to be on the inside network.
Procedure

Step 1  Create a network object for the dynamic NAT pool to which you want to translate the inside addresses.

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

Step 2  Create a network object for the inside network.

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

Step 3  Enable dynamic NAT for the inside network using the dynamic NAT pool object.

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

Step 4  Create a network object for the outside web server.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

Step 5  Configure static NAT for the web server.
Inside Load Balancer with Multiple Mapped Addresses (Static NAT, One-to-Many)

The following example shows an inside load balancer that is translated to multiple IP addresses. When an outside host accesses one of the mapped IP addresses, it is untranslated to the single load balancer address. Depending on the URL requested, it redirects traffic to the correct web server.

*Figure 30: Static NAT with One-to-Many for an Inside Load Balancer*

---

**Procedure**

**Step 1**
Create a network object for the addresses to which you want to map the load balancer.

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

**Step 2**
Create a network object for the load balancer.

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27

**Step 3** Configure static NAT for the load balancer applying the range object.

hostname(config-network-object)# nat (inside,outside) static myPublicIPs

---

**Single Address for FTP, HTTP, and SMTP (Static NAT-with-Port-Translation)**

The following static NAT-with-port-translation example provides a single address for remote users to access FTP, HTTP, and SMTP. These servers are actually different devices on the real network, but for each server, you can specify static NAT-with-port-translation rules that use the same mapped IP address, but different ports.

*Figure 31: Static NAT-with-Port-Translation*

**Procedure**

**Step 1** Create a network object for the FTP server and configure static NAT with port translation, mapping the FTP port to itself.
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp

Step 2 Create a network object for the HTTP server and configure static NAT with port translation, mapping the HTTP port to itself.

hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp http

Step 3 Create a network object for the SMTP server and configure static NAT with port translation, mapping the SMTP port to itself.

hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp smtp

Examples for Twice NAT

This section includes the following configuration examples:

Different Translation Depending on the Destination (Dynamic Twice PAT)

The following figure shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129:port. When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130:port.
Figure 32: Twice NAT with Different Destination Addresses

Procedure

Step 1  Add a network object for the inside network:

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

Step 2  Add a network object for the DMZ network 1:

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

Step 3  Add a network object for the PAT address:

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

Step 4  Configure the first twice NAT rule:

```
hostname(config)# nat (inside, dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the real and mapped destination addresses.
**Step 5**  Add a network object for the DMZ network 2:

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

**Step 6**  Add a network object for the PAT address:

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

**Step 7**  Configure the second twice NAT rule:

**Example:**

```
hostname(config)# nat (inside, dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

---

**Different Translation Depending on the Destination Address and Port (Dynamic PAT)**

The following figure 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 Telnet services, the real address is translated to 209.165.202.129:port. When the host accesses the same server for web services, the real address is translated to 209.165.202.130:port.

*Figure 33: Twice NAT with Different Destination Ports*
**Procedure**

**Step 1** Add a network object for the inside network:

```conf
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

**Step 2** Add a network object for the Telnet/Web server:

```conf
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

**Step 3** Add a network object for the PAT address when using Telnet:

```conf
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

**Step 4** Add a service object for Telnet:

```conf
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

**Step 5** Configure the first twice NAT rule:

```conf
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

Because you do not want to translate the destination address or port, you need to configure identity NAT for them by specifying the same address for the real and mapped destination addresses, and the same port for the real and mapped service.

**Step 6** Add a network object for the PAT address when using HTTP:

```conf
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

**Step 7** Add a service object for HTTP:

```conf
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

**Step 8** Configure the second twice NAT rule:

```conf
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```
Example: Twice NAT with Destination Address Translation

The following figure shows a remote host connecting to a mapped host. The mapped host has a twice 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 34: Twice Static NAT with Destination Address Translation

NAT in Routed and Transparent Mode

You can configure NAT in both routed and transparent firewall mode. The following sections describe typical usage for each firewall mode.

NAT in Routed Mode

The following figure shows a typical NAT example in routed mode, with a private network on the inside.
1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is translated to a mapped address, 209.165.201.10.

2. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the ASA receives the packet because the ASA performs proxy ARP to claim the packet.

3. The ASA then changes the translation of the mapped address, 209.165.201.10, back to the real address, 10.1.2.27, before sending it to the host.

**NAT in Transparent Mode or Within a Bridge Group**

Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks. It can perform a similar function within a bridge group in routed mode.

NAT in transparent mode, or in routed mode between members of the same bridge group, has the following requirements and limitations:

- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.

- ARP inspection is not supported. Moreover, if for some reason a host on one side of the ASA sends an ARP request to a host on the other side of the ASA, and the initiating host real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.

- Translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

The following figure shows a typical NAT scenario in transparent mode, with the same network on the inside and outside interfaces. The transparent firewall in this scenario is performing the NAT service so that the upstream router does not have to perform NAT.
1. When the inside host at 10.1.1.75 sends a packet to a web server, the real source address of the packet, 10.1.1.75, is changed to a mapped address, 209.165.201.15.

2. When the server responds, it sends the response to the mapped address, 209.165.201.15, and the ASA receives the packet because the upstream router includes this mapped network in a static route directed to the ASA management IP address.

3. The ASA then undoes the translation of the mapped address, 209.165.201.15, back to the real address, 10.1.1.75. Because the real address is directly-connected, the ASA sends it directly to the host.

4. For host 192.168.1.2, the same process occurs, except for returning traffic, the ASA looks up the route in its routing table and sends the packet to the downstream router at 10.1.1.3 based on the ASA static route for 192.168.1.0/24.

Routing NAT Packets

The ASA needs to be the destination for any packets sent to the mapped address. The ASA also needs to determine the egress interface for any packets it receives destined for mapped addresses. This section describes how the ASA handles accepting and delivering packets with NAT.
Mapped Addresses and Routing

When you translate the real address to a mapped address, the mapped address you choose determines how to configure routing, if necessary, for the mapped address.

See additional guidelines about mapped IP addresses in Additional Guidelines for NAT, on page 208.

The following topics explain the mapped address types.

Addresses on the Same Network as the Mapped Interface

If you use addresses on the same network as the destination (mapped) interface, the ASA uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the ASA does not have to be the gateway for any additional networks. This solution is ideal if the outside network contains an adequate number of free addresses, a consideration if you are using a 1:1 translation like dynamic NAT or static NAT. Dynamic PAT greatly extends the number of translations you can use with a small number of addresses, so even if the available addresses on the outside network is small, this method can be used. For PAT, you can even use the IP address of the mapped interface.

Note

If you configure the mapped interface to be any interface, and you specify a mapped address on the same network as one of the mapped interfaces, then if an ARP request for that mapped address comes in on a different interface, then you need to manually configure an ARP entry for that network on the ingress interface, specifying its MAC address. Typically, if you specify any interface for the mapped interface, then you use a unique network for the mapped addresses, so this situation would not occur. Configure ARP using the `arp` command.

Addresses on a Unique Network

If you need more addresses than are available on the destination (mapped) interface network, you can identify addresses on a different subnet. The upstream router needs a static route for the mapped addresses that points to the ASA.

Alternatively for routed mode, you can configure a static route on the ASA for the mapped addresses using any IP address on the destination network as the gateway, and then redistribute the route using your routing protocol. For example, if you use NAT for the inside network (10.1.1.0/24) and use the mapped IP address 209.165.201.5, then you can configure a static route for 209.165.201.5 255.255.255.255 (host address) to the 10.1.1.99 gateway that can be redistributed.

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

For transparent mode, if the real host is directly-connected, configure the static route on the upstream router to point to the ASA: specify the bridge group IP address. For remote hosts in transparent mode, in the static route on the upstream router, you can alternatively specify the downstream router IP address.

The Same Address as the Real Address (Identity NAT)

The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. You can also disable proxy ARP for regular static NAT if desired, in which case you need to be sure to have proper routes on the upstream router.
Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues. For example, if you configure a broad identity NAT rule for “any” IP address, then leaving proxy ARP enabled can cause problems for hosts on the network directly connected to the mapped interface. In this case, when a host on the mapped network wants to communicate with another host on the same network, then the address in the ARP request matches the NAT rule (which matches “any” address). The ASA will then proxy ARP for the address, even though the packet is not actually destined for the ASA. (Note that this problem occurs even if you have a twice NAT rule; although the NAT rule must match both the source and destination addresses, the proxy ARP decision is made only on the “source” address). If the ASA ARP response is received before the actual host ARP response, then traffic will be mistakenly sent to the ASA.

Figure 37: Proxy ARP Problems with Identity NAT

In rare cases, you need proxy ARP for identity NAT; for example for virtual Telnet. When using AAA for network access, a host needs to authenticate with the ASA using a service like Telnet before any other traffic can pass. You can configure a virtual Telnet server on the ASA to provide the necessary login. When accessing the virtual Telnet address from the outside, you must configure an identity NAT rule for the address specifically for the proxy ARP functionality. Due to internal processes for virtual Telnet, proxy ARP lets the ASA keep traffic destined for the virtual Telnet address rather than send the traffic out the source interface according to the NAT rule. (See the following figure).

Figure 38: Proxy ARP and Virtual Telnet
Transparent Mode Routing Requirements for Remote Networks

When you use NAT in transparent mode, some types of traffic require static routes. See the general operations configuration guide for more information.

Determining the Egress Interface

When you use NAT and the ASA receives traffic for a mapped address, then the ASA untranslates the destination address according to the NAT rule, and then it sends the packet on to the real address. The ASA determines the egress interface for the packet in the following ways:

- Bridge group interfaces in Transparent mode or Routed Mode—The ASA determines the egress interface for the real address by using the NAT rule; you must specify the source and destination bridge group member interfaces as part of the NAT rule.

- Regular interfaces in Routed mode—The ASA determines the egress interface in one of the following ways:
  - You configure the interface in the NAT rule—The ASA uses the NAT rule to determine the egress interface. However, you have the option to always use a route lookup instead. In certain scenarios, a route lookup override is required.
  - You do not configure the interface in the NAT rule—The ASA uses a route lookup to determine the egress interface.

The following figure shows the egress interface selection method in routed mode. In almost all cases, a route lookup is equivalent to the NAT rule interface, but in some configurations, the two methods might differ.

Figure 39: Routed Mode Egress Interface Selection with NAT

The following topics explain NAT usage with the various types of VPN.

NAT for VPN

The following topics explain NAT usage with the various types of VPN.
NAT and Remote Access VPN

The following figure shows both an inside server (10.1.1.6) and a VPN client (209.165.201.10) accessing the Internet. Unless you configure split tunneling for the VPN client (where only specified traffic goes through the VPN tunnel), then Internet-bound VPN traffic must also go through the ASA. When the VPN traffic enters the ASA, the ASA decrypts the packet; the resulting packet includes the VPN client local address (10.3.3.10) as the source. For both inside and VPN local networks, you need a public IP address provided by NAT to access the Internet. The below example uses interface PAT rules. To allow the VPN traffic to exit the same interface it entered, you also need to enable intra-interface communication (also known as “hairpin” networking).

Figure 40: Interface PAT for Internet-Bound VPN Traffic (Intra-Interface)

The following figure shows a VPN client that wants to access an inside mail server. Because the ASA expects traffic between the inside network and any outside network to match the interface PAT rule you set up for Internet access, traffic from the VPN client (10.3.3.10) to the SMTP server (10.1.1.6) will be dropped due to a reverse path failure: traffic from 10.3.3.10 to 10.1.1.6 does not match a NAT rule, but returning traffic from 10.1.1.6 to 10.3.3.10 should match the interface PAT rule for outgoing traffic. Because forward and reverse flows do not match, the ASA drops the packet when it is received. To avoid this failure, you need to exempt the inside-to-VPN client traffic from the interface PAT rule by using an identity NAT rule between those networks. Identity NAT simply translates an address to the same address.
See the following sample NAT configuration for the above network:

! Enable hairpin for non-split-tunneled VPN client traffic:
  same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
  object network vpn_local
  subnet 10.3.3.0 255.255.255.0
  nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
  object network inside_nw
  subnet 10.1.1.0 255.255.255.0
  nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
  nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local

---

**NAT and Site-to-Site VPN**

The following figure shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface PAT rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San
Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT simply translates an address to the same address.

**Figure 42: Interface PAT and Identity NAT for Site-to-Site VPN**

The following figure shows a VPN client connected to Firewall1 (Boulder), with a Telnet request for a server (10.2.2.78) accessible over a site-to-site tunnel between Firewall1 and Firewall2 (San Jose). Because this is a hairpin connection, you need to enable intra-interface communication, which is also required for non-split-tunneled Internet-bound traffic from the VPN client. You also need to configure identity NAT between the VPN client and the Boulder & San Jose networks, just as you would between any networks connected by VPN to exempt this traffic from outbound NAT rules.

**Figure 43: VPN Client Access to Site-to-Site VPN**

See the following sample NAT configuration for Firewall1 (Boulder) for the second example:
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
   subnet 10.3.3.0 255.255.255.0
   nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
   subnet 10.1.1.0 255.255.255.0
   nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
   subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
   nat (inside,outside) source static boulder_inside boulder_inside
   destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
   nat (inside,outside) source static boulder_inside boulder_inside
   destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
   nat (inside,outside) source static sanjose_inside sanjose_inside
   destination static vpn_local vpn_local

See the following sample NAT configuration for Firewall2 (San Jose):

! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
   subnet 10.2.2.0 255.255.255.0
   nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
   subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
   subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
   nat (inside,outside) source static sanjose_inside sanjose_inside
   destination static boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
   nat (inside,outside) source static sanjose_inside sanjose_inside
   destination static vpn_local vpn_local
NAT and VPN Management Access

When using VPN, you can allow management access to an interface other than the one from which you entered the ASA (see the management-access command). For example, if you enter the ASA from the outside interface, the management-access feature lets you connect to the inside interface using ASDM, SSH, Telnet, or SNMP; or you can ping the inside interface.

The following figure shows a VPN client Telnetting to the ASA inside interface. When you use a management-access interface, and you configure identity NAT according to NAT and Remote Access VPN, on page 264 or NAT and Site-to-Site VPN, on page 265, you must configure NAT with the route lookup option. Without route lookup, the ASA sends traffic out the interface specified in the NAT command, regardless of what the routing table says; in the below example, the egress interface is the inside interface. You do not want the ASA to send the management traffic out to the inside network; it will never return to the inside interface IP address. The route lookup option lets the ASA send the traffic directly to the inside interface IP address instead of to the inside network. For traffic from the VPN client to a host on the inside network, the route lookup option will still result in the correct egress interface (inside), so normal traffic flow is not affected. See the Determining the Egress Interface, on page 263 for more information about the route lookup option.

Figure 44: VPN Management Access

See the following sample NAT configuration for the above network:

! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside, outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside, outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside, inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup

Troubleshooting NAT and VPN

See the following monitoring tools for troubleshooting NAT issues with VPN:

- Packet tracer—When used correctly, a packet tracer shows which NAT rules a packet is hitting.
- show nat detail—Shows hit counts and untranslated traffic for a given NAT rule.
- show conn all—Lets you see active connections including to and from the box traffic.

To familiarize yourself with a non-working configuration vs. a working configuration, you can perform the following steps:

1. Configure VPN without identity NAT.
2. Enter show nat detail and show conn all.
3. Add the identity NAT configuration.
4. Repeat show nat detail and show conn all.

Translating IPv6 Networks

In cases where you need to pass traffic between IPv6-only and IPv4-only networks, you need to use NAT to convert between the address types. Even with two IPv6 networks, you might want to hide internal addresses from the outside network.

You can use the following translation types with IPv6 networks:

- NAT64, NAT46—Translates IPv6 packets into IPv4 and vice versa. You need to define two policies, one for the IPv6 to IPv4 translation, and one for the IPv4 to IPv6 translation. Although you can accomplish this with a single twice NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a twice NAT rule when you specify a destination, creating two network object NAT rules is the better solution.

Note
NAT46 supports static mappings only.
• NAT66—Translates IPv6 packets to a different IPv6 address. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.

---

**Note**

NAT64 and NAT 46 are possible on standard routed interfaces only. NAT66 is possible on both routed and bridge group member interfaces.

---

**NAT64/46: Translating IPv6 Addresses to IPv4**

When traffic goes from an IPv6 network to an IPv4-only network, you need to convert the IPv6 address to IPv4, and return traffic from IPv4 to IPv6. You need to define two address pools, an IPv4 address pool to bind IPv6 addresses in the IPv4 network, and an IPv6 address pool to bind IPv4 addresses in the IPv6 network.

• The IPv4 address pool for the NAT64 rule is normally small and typically might not have enough addresses to map one-to-one with the IPv6 client addresses. Dynamic PAT might more easily meet the possible large number of IPv6 client addresses compared to dynamic or static NAT.

• The IPv6 address pool for the NAT46 rule can be equal to or larger than the number of IPv4 addresses to be mapped. This allows each IPv4 address to be mapped to a different IPv6 address. NAT46 supports static mappings only, so you cannot use dynamic PAT.

You need to define two policies, one for the source IPv6 network, and one for the destination IPv4 network. Although you can accomplish this with a single twice NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a twice NAT rule when you specify a destination, creating two network object NAT rules is the better solution.

**NAT64/46 Example: Inside IPv6 Network with Outside IPv4 Internet**

Following is a typical example where you have an inside IPv6-only network, but there are some IPv4-only services on the outside Internet that internal users need.
In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network. You enable DNS rewrite on the NAT46 rule, so that replies from the external DNS server can be converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

Following is a typical sequence for a web request where a client at 2001:DB8::100 on the internal IPv6 network tries to open www.example.com.

1. The client’s computer sends a DNS request to the DNS server at 2001:DB8::D1A5:CA81. The NAT rules make the following translations to the source and destination in the DNS request:
   - 2001:DB8::100 to a unique port on 209.165.201.1 (The NAT64 interface PAT rule.)
   - 2001:DB8::D1A5:CA81 to 209.165.202.129 (The NAT46 rule. D1A5:CA81 is the IPv6 equivalent of 209.165.202.129.)

2. The DNS server responds with an A record indicating that www.example.com is at 209.165.200.225. The NAT46 rule, with DNS rewrite enabled, converts the A record to the IPv6-equivalent AAAA record, and translates 209.165.200.225 to 2001:db8:D1A5:C8E1 in the AAAA record. In addition, the source and destination addresses in the DNS response are untranslated:
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100

3. The IPv6 client now has the IP address of the web server, and makes an HTTP request to www.example.com at 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) The source and destination of the HTTP request are translated:
   - 2001:DB8::100 to a unique port on 209.156.101.54 (The NAT64 interface PAT rule.)
   - 2001:db8:D1A5:C8E1 to 209.165.200.225 (The NAT46 rule.)
The following procedure explains how to configure this example.

**Procedure**

**Step 1** Create a network object for the inside IPv6 network and add the NAT64 rule.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside, outside) dynamic interface
```

With this rule, any traffic from the 2001:db8::/96 subnet on the inside interface going to the outside interface gets a NAT64 PAT translation using the IPv4 address of the outside interface.

**Step 2** Create a network object for the IPv6 translated network for the outside IPv4 network and add the NAT46 rule.

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside, inside) static 2001:db8::/96 dns
```

With this rule, any IPv4 address on the outside network coming to the inside interface is translated to an address on the 2001:db8::/96 network using the embedded IPv4 address method. In addition, DNS responses are converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

---

**NAT66: Translating IPv6 Addresses to Different IPv6 Addresses**

When going from an IPv6 network to another IPv6 network, you can translate the addresses to different IPv6 addresses on the outside network. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.

Because you are not translating between different address types, you need a single rule for NAT66 translations. You can easily model these rules using network object NAT. However, if you do not want to allow returning traffic, you can make the static NAT rule unidirectional using twice NAT only.

**NAT66 Example, Static Translation between Networks**

You can configure a static translation between IPv6 address pools using network object NAT. The following example explains how to convert inside addresses on the 2001:db8:122:2091::/96 network to outside addresses on the 2001:db8:122:2999::/96 network.
Procedure

Create the network object for the inside IPv6 network and add the static NAT rule.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a static NAT66 translation to an address on the 2001:db8:122:2999::/96 network.

**NAT66 Example, Simple IPv6 Interface PAT**

A simple approach for implementing NAT66 is to dynamically assign internal addresses to different ports on the outside interface IPv6 address.

When you configure an interface PAT rule for NAT66, all the global addresses that are configured on that interface are used for PAT mapping. Link-local or site-local addresses for the interface are not used for PAT.
Procedure

Create the network object for the inside IPv6 network and add the dynamic PAT rule.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a NAT66 PAT translation to one of the IPv6 global addresses configured for the outside interface.

---

**Rewriting DNS Queries and Responses Using NAT**

You might need to configure the ASA 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 rule. DNS modification is also known as DNS doctoring.

This feature rewrites the address in DNS queries and replies that match a NAT rule (for example, the A record for IPv4, the AAAA record for IPv6, or the PTR record for reverse DNS queries). For DNS replies traversing from a mapped interface to any other interface, the record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the record is rewritten from the real value to the mapped value.

Following are the main circumstances when you would need to configure DNS rewrite on a NAT rule.
Network Address Translation

- The rule is NAT64 or NAT46, and the DNS server is on the outside network. You need DNS rewrite to convert between DNS A records (for IPv4) and AAAA records (for IPv6).
- The DNS server is on the outside, clients are on the inside, and some of the fully-qualified domain names that the clients use resolve to other inside hosts.
- The DNS server is on the inside and responds with private IP addresses, clients are on the outside, and the clients access fully-qualified domain names that point to servers that are hosted on the inside.

DNS Rewrite Limitations

Following are some limitations with DNS rewrite:

- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A or AAAA record, and the PAT rule to use is ambiguous.
- If you configure a twice NAT rule, you cannot configure DNS modification if you specify the destination address as well as the source address. These kinds of rules can potentially have a different translation for a single address when going to A vs. B. Therefore, the ASA cannot accurately match the IP address inside the DNS reply to the correct twice NAT rule; the DNS reply does not contain information about which source/destination address combination was in the packet that prompted the DNS request.
- You must enable DNS application inspection with DNS NAT rewrite enabled for NAT rules to rewrite DNS queries and responses. By default, DNS inspection with DNS NAT rewrite enabled is globally applied, so you probably do not need to change the inspection configuration.
- DNS rewrite is actually done on the xlate entry, not the NAT rule. Thus, if there is no xlate for a dynamic rule, rewrite cannot be done correctly. The same problem does not occur for static NAT.
- DNS rewrite does not rewrite DNS Dynamic Update messages (opcode 5).

The following topics provide examples of DNS rewrite in NAT rules.

DNS Reply Modification, DNS Server on Outside

The following figure shows a DNS server that is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure NAT to statically translate the ftp.cisco.com real address (10.1.3.14) to a mapped address (209.165.201.10) that is visible on the outside network.

In this case, you want to enable DNS reply modification on this static rule so that inside users who have access to ftp.cisco.com using the real address receive the real address from the DNS server, and not the mapped address.

When an inside host sends a DNS request for the address of ftp.cisco.com, the DNS server replies with the mapped address (209.165.201.10). The system refers to the static rule for the inside server and translates the address inside the DNS reply to 10.1.3.14. If you do not enable DNS reply modification, then the inside host attempts to send traffic to 209.165.201.10 instead of accessing ftp.cisco.com directly.
**Procedure**

**Step 1**  
Create a network object for the FTP server.

```
hostname(config)# object network FTP_SERVER  
hostname(config-network-object)# host 10.1.3.14
```

**Step 2**  
Configure static NAT with DNS modification.

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

**DNS Reply Modification, DNS Server, Host, and Server on Separate Networks**

The following figure shows a user on the inside network requesting the IP address for ftp.cisco.com, which is on the DMZ network, from an outside DNS server. The DNS server replies with the mapped address (209.165.201.10) according to the static rule between outside and DMZ even though the user is not on the DMZ network. The ASA translates the address inside the DNS reply to 10.1.3.14.
If the user needs to access ftp.cisco.com using the real address, then no further configuration is required. If there is also a static rule between the inside and DMZ, then you also need to enable DNS reply modification on this rule. The DNS reply will then be modified two times. In this case, the ASA again translates the address inside the DNS reply to 192.168.1.10 according to the static rule between inside and DMZ.

Figure 45: DNS Reply Modification, DNS Server, Host, and Server on Separate Networks

DNS Reply Modification, DNS Server on Host Network

The following figure shows an FTP server and DNS server on the outside. The system has a static translation for the outside server. In this case, when an inside user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.20.10. Because you want inside users to use the mapped address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.
Procedure

**Step 1**
Create a network object for the FTP server.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

**Step 2**
Configure static NAT with DNS modification.

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

### DNS64 Reply Modification

The following figure shows an FTP server and DNS server on the outside IPv4 network. The system has a static translation for the outside server. In this case, when an inside IPv6 user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.200.225.

Because you want inside users to use the mapped address for ftp.cisco.com (2001:DB8::D1A5:C8E1, where D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225) you need to configure DNS reply modification for
the static translation. This example also includes a static NAT translation for the DNS server, and a PAT rule for the inside IPv6 hosts.

**Procedure**

**Step 1** Create a network object for the FTP server and configure static NAT with DNS modification. Because this is a one-to-one translation, include the `net-to-net` option for NAT46.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128 net-to-net dns
```

**Step 2** Create a network object for the DNS server and configure static NAT. Include the `net-to-net` option for NAT46.

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128 net-to-net
```

**Step 3** Configure an IPv4 PAT pool for translating the inside IPv6 network.
Example:

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

**Step 4** Create a network object for the inside IPv6 network, and configure dynamic NAT with a PAT pool.

```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

**PTR Modification, DNS Server on Host Network**

The following figure shows an FTP server and DNS server on the outside. The ASA has a static translation for the outside server. In this case, when an inside user performs a reverse DNS lookup for 10.1.2.56, the ASA modifies the reverse DNS query with the real address, and the DNS server responds with the server name, ftp.cisco.com.

*Figure 46: PTR Modification, DNS Server on Host Network*
PART IV

Service Policies and Application Inspection

• Service Policy, on page 283
• Getting Started with Application Layer Protocol Inspection, on page 307
• Inspection of Basic Internet Protocols, on page 329
• Inspection for Voice and Video Protocols, on page 369
• Inspection for Mobile Networks, on page 393
CHAPTER 13

Service Policy

Service policies using Modular Policy Framework provide a consistent and flexible way to configure ASA 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. A service policy consists of multiple actions or rules applied to an interface or applied globally.

- About Service Policies, on page 283
- Guidelines for Service Policies, on page 290
- Defaults for Service Policies, on page 291
- Configure Service Policies, on page 293
- Monitoring Service Policies, on page 301
- Examples for Service Policies (Modular Policy Framework), on page 301
- History for Service Policies, on page 304

About Service Policies

The following topics describe how service policies work.

The Components of a Service Policy

The point of service policies is to apply advanced services to the traffic you are allowing. Any traffic permitted by access rules can have service policies applied, and thus receive special processing, such as being redirected to a service module or having application inspection applied.

You can have these types of service policy:

- One global policy that gets applied to all interfaces.
- One service policy applied per interface. The policy can be a mix of classes for traffic going through the device and management traffic directed at the ASA interface rather than going through it.

Each service policy is composed of the following elements:

1. Service policy map, which is the ordered set of rules, and is named on the service-policy command. In ASDM, the policy map is represented as a folder on the Service Policy Rules page.
2. Rules, each rule being a class command within the service policy map and the commands associated with the class command. In ASDM, each rule is shown on a separate row, and the name of the rule is the class name.
The **class** command defines the traffic matching criteria for the rule.

The commands associated with class, such as **inspect**, **set connection timeout**, and so forth, define the services and constraints to apply to matching traffic. Note that inspect commands can point to inspection policy maps, which define actions to apply to inspected traffic. Keep in mind that inspection policy maps are not the same as service policy maps.

The following example compares how service policies appear in the CLI with how they appear in ASDM. Note that there is not a one-to-one mapping between the figure call-outs and lines in the CLI.

The following CLI is generated by the rules shown in the figure above.

```cli
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
deny version 1
deny version 2
deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
parameters
  rtp-conformance enforce-payloadtype
  no traffic-non-sip
  software-version action mask log
  uri-non-sip action mask log
  state-checking action drop-connection log
  max-forwards-validation action drop log
  strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
```

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10
class-map inside-class1
    match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
    reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside

Features Configured with Service Policies

The following table lists the features you configure using service policies.

Table 10: Features Configured with Service Policies

<table>
<thead>
<tr>
<th>Feature</th>
<th>For Through Traffic?</th>
<th>For Management Traffic?</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application inspection (multiple types)</td>
<td>All except RADIUS accounting</td>
<td>RADIUS accounting only</td>
<td>• Getting Started with Application Layer Protocol Inspection, on page 307.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Inspection of Basic Internet Protocols, on page 329.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Inspection for Voice and Video Protocols, on page 369.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Inspection for Mobile Networks, on page 393.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ASA and Cisco Cloud Web Security, on page 165.</td>
</tr>
<tr>
<td>ASA IPS</td>
<td>Yes</td>
<td>No</td>
<td>See the ASA IPS quick start guide.</td>
</tr>
<tr>
<td>ASA CX</td>
<td>Yes</td>
<td>No</td>
<td>See the ASA CX quick start guide.</td>
</tr>
<tr>
<td>ASA FirePOWER (ASA SFR)</td>
<td>Yes</td>
<td>No</td>
<td>ASA FirePOWER Module, on page 115.</td>
</tr>
<tr>
<td>NetFlow Secure Event Logging filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>See the NetFlow implementation guide.</td>
</tr>
<tr>
<td>QoS input and output policing</td>
<td>Yes</td>
<td>No</td>
<td>Quality of Service, on page 465.</td>
</tr>
<tr>
<td>QoS standard priority queue</td>
<td>Yes</td>
<td>No</td>
<td>Quality of Service, on page 465.</td>
</tr>
</tbody>
</table>
### 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 enters (or exits, depending on the feature) the interface to which you apply the policy map is affected. See the following table for the directionality of each feature.

#### Table 11: Feature Directionality

<table>
<thead>
<tr>
<th>Feature</th>
<th>Single Interface Direction</th>
<th>Global Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application inspection (multiple types)</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>ASA CX</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>ASA CX authentication proxy</td>
<td>Ingress</td>
<td>Ingress</td>
</tr>
<tr>
<td>ASA FirePOWER (ASA SFR)</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>ASA IPS</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>NetFlow Secure Event Logging filtering</td>
<td>N/A</td>
<td>Ingress</td>
</tr>
<tr>
<td>QoS input policing</td>
<td>Ingress</td>
<td>Ingress</td>
</tr>
<tr>
<td>QoS output policing</td>
<td>Egress</td>
<td>Egress</td>
</tr>
</tbody>
</table>
Feature Matching Within a Service Policy

A packet matches class maps in a policy map for a given interface according to the following rules:

1. A packet can match only one class map in the policy map for each feature type.

2. When the packet matches a class map for a feature type, the ASA does not attempt to match it to any subsequent class maps for that feature type.

3. If the packet matches a subsequent class map for a different feature type, however, then the ASA also applies the actions for the subsequent class map, if supported. See Incompatibility of Certain Feature Actions, on page 288 for more information about unsupported combinations.

Note
Application inspection includes multiple inspection types, and most are mutually exclusive. For inspections that can be combined, each inspection is considered to be a separate feature.

Examples of Packet Matching

For example:

- If a packet matches a class map for connection limits, and also matches a class map for an application inspection, then both actions are applied.

- If a packet matches a class map for HTTP inspection, but also matches another class map that includes HTTP inspection, then the second class map actions are not applied.

- If a packet matches a class map for HTTP inspection, but also matches another class map that includes FTP inspection, then the second class map actions are not applied because HTTP and FTP inspections cannot be combined.

- If a packet matches a class map for HTTP inspection, but also matches another class map that includes IPv6 inspection, then both actions are applied because the IPv6 inspection can be combined with any other type of inspection.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Single Interface Direction</th>
<th>Global Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS standard priority queue</td>
<td>Egress</td>
<td>Egress</td>
</tr>
<tr>
<td>TCP and UDP connection limits</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>and timeouts, and TCP sequence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>number randomization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP normalization</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>TCP state bypass</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
<tr>
<td>User statistics for Identity Firewall</td>
<td>Bidirectional</td>
<td>Ingress</td>
</tr>
</tbody>
</table>
Order in Which Multiple Feature Actions are Applied

The order in which different types of actions in a policy map are performed is independent of the order in which the actions appear in the policy map.

Actions are performed in the following order:

1. QoS input policing
2. TCP normalization, TCP and UDP connection limits and timeouts, TCP sequence number randomization, and TCP state bypass.

Note

When a the ASA 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. Application inspections that can be combined with other inspections:
   1. IPv6
   2. IP options
   3. WAAS

4. Application inspections that cannot be combined with other inspections. See Incompatibility of Certain Feature Actions, on page 288 for more information.

   5. ASA IPS
   6. ASA CX
   7. ASA FirePOWER (ASA SFR)
   8. QoS output policing
   9. QoS standard priority queue

Note

NetFlow Secure Event Logging filtering and User statistics for Identity Firewall are order-independent.

Incompatibility of Certain Feature Actions

Some features are not compatible with each other for the same traffic. The following list might not include all incompatibilities; for information about compatibility of each feature, see the chapter or section for the feature:

- You cannot configure QoS priority queuing and QoS policing for the same set of traffic.
- Most inspections should not be combined with another inspection, so the ASA only applies one inspection if you configure multiple inspections for the same traffic. HTTP inspection can be combined with the Cloud Web Security inspection. Other exceptions are listed in Order in Which Multiple Feature Actions are Applied, on page 288.
• You cannot configure traffic to be sent to multiple modules, such as the ASA CX and ASA IPS.
• HTTP inspection is not compatible with ASA CX or ASA FirePOWER.
• Cloud Web Security is not compatible with ASA CX or ASA FirePOWER.

The **match default-inspection-traffic** command, which is used in the default global policy, is a special CLI shortcut to match the default ports for all inspections. When used in a policy map, this class map 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 ASA, then the ASA applies the TFTP inspection; when TCP traffic for port 21 arrives, then the ASA applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map. Normally, the ASA does not use the port number to determine which inspection to apply, thus giving you the flexibility to apply inspections to non-standard ports, for example.

This traffic class does not include the default ports for Cloud Web Security inspection (80 and 443).

An example of a misconfiguration is if you configure multiple inspections in the same policy map and do not use the default-inspection-traffic shortcut. In the first example, traffic destined to port 21 is mistakenly configured for both FTP and HTTP inspection. In the second example, traffic destined to port 80 is mistakenly configured for both FTP and HTTP inspection. In both cases of misconfiguration examples, only the FTP inspection is applied, because FTP comes before HTTP in the order of inspections applied.

**Example 1: Misconfiguration for FTP packets: HTTP Inspection Also Configured**

```plaintext
class-map ftp
  match port tcp eq 21
class-map http
  match port tcp eq 21 [it should be 80]
policy-map test
  class ftp
    inspect ftp
  class http
    inspect http
```

**Example 2: Misconfiguration for HTTP packets: FTP Inspection Also Configured**

```plaintext
class-map ftp
  match port tcp eq 80 [it should be 21]
class-map http
  match port tcp eq 80
policy-map test
  class ftp
    inspect ftp
  class http
    inspect http
```

**Feature Matching 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 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.

Guidelines for Service Policies

Inspection Guidelines

There is a separate topic that provides detailed guidelines for application inspection service policies. See Guidelines for Application Inspection, on page 309.

IPv6 Guidelines

Supports IPv6 for the following features:

• Application inspection for several, but not all, protocols. For details, see Guidelines for Application Inspection, on page 309.
• ASA IPS
• ASA CX
• ASA FirePOWER
• NetFlow Secure Event Logging filtering
• SCTP state bypass
• TCP and UDP connection limits and timeouts, TCP sequence number randomization
• TCP normalization
• TCP state bypass
• User statistics for Identity Firewall

Class Map (Traffic Class) Guidelines

The maximum number of class maps (traffic classes) of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

• Layer 3/4 class maps (for through traffic and management traffic).
• Inspection class maps
• Regular expression class maps
• **match** commands used directly underneath an inspection policy map

This limit also includes default class maps of all types, limiting user-configured class maps to approximately 235.

**Policy Map Guidelines**

See the following guidelines for using policy maps:

• You can only assign one policy map per interface. However you can create up to 64 policy maps in the configuration.

• You can apply the same policy map to multiple interfaces.

• You can identify up to 63 Layer 3/4 class maps in a Layer 3/4 policy map.

• For each class map, you can assign multiple actions from one or more feature types, if supported. See **Incompatibility of Certain Feature Actions**, on page 288.

**Service Policy Guidelines**

• Interface service policies on ingress interfaces 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 normalization, then both FTP inspection and TCP normalization are applied to the interface. However, if you have a global policy with FTP inspection, and an ingress interface policy with FTP inspection, then only the ingress interface policy FTP inspection is applied to that interface. If no ingress or global policy implements a feature, then an interface service policy on the egress interface that specifies the feature is applied.

• You can only apply one global policy. For example, you cannot create a global policy that includes feature set 1, and a separate global policy that includes feature set 2. All features must be included in a single policy.

• When you make service policy changes to the configuration, all new connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. Output for the **show** command will not include data about the old connections.

For example, if you remove a QoS service policy from an interface, then add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output.

To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. Use the **clear conn** or **clear local-host** commands.

**Defaults for Service Policies**

The following topics describe the default settings for service policies and the Modular Policy Framework.
Default Service Policy Configuration

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 for a particular feature.)

The default policy includes the following application inspections:

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

The default policy configuration includes the following commands:

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225 _default_h323_map
 inspect h323 ras _default_h323_map
 inspect ip-options _default_ip_options_map
 inspect netbios
 inspect rsh
 inspect rtsp
```
Default Class Maps (Traffic Classes)

The configuration includes a default Layer 3/4 class map (traffic class) that the ASA uses in the default global policy called default-inspection-traffic; it matches the default inspection traffic. This class, which is used in the default global policy, is a special shortcut to match the default ports for all inspections.

When used in a policy, this class 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 ASA, then the ASA applies the TFTP inspection; when TCP traffic for port 21 arrives, then the ASA applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map. Normally, the ASA does not use the port number to determine which inspection to apply, thus giving you the flexibility to apply inspections to non-standard ports, for example.

```plaintext
class-map inspection_default
  match default-inspection-traffic
```

Another class map that exists in the default configuration is called class-default, and it matches all traffic. This class map appears at the end of all Layer 3/4 policy maps and essentially tells the ASA to not perform any actions on all other traffic. You can use the class-default class if desired, rather than making your own `match any` class map. In fact, some features are only available for class-default.

```plaintext
class-map class-default
  match any
```

Configure Service Policies

To configure service policies using the Modular Policy Framework, perform the following steps:

Procedure

**Step 1** Identify the traffic on which you want to act by creating Layer 3/4 class maps, as described in Identify Traffic (Layer 3/4 Class Maps), on page 295.

For example, you might want to perform actions on all traffic that passes through the ASA; or you might only want to perform certain actions on traffic from 10.1.1.0/24 to any destination address.
Step 2  Optionally, perform additional actions on some inspection traffic.

If one of the actions you want to perform is application inspection, and you want to perform additional actions on some inspection traffic, then create an inspection policy map. The inspection policy map identifies the traffic and specifies what to do with it.

For example, you might want to drop all HTTP requests with a body length greater than 1000 bytes.

You can create a self-contained inspection policy map that identifies the traffic directly with match commands, or you can create an inspection class map for reuse or for more complicated matching. For example, you could match text within a inspected packets using a regular expression or a group of regular expressions (a regular expression class map), and target actions based on narrower criteria. For example, you might want to drop all HTTP requests with a URL including the text “example.com.”

Step 3  Define the actions you want to perform on each Layer 3/4 class map by creating a Layer 3/4 policy map, as described in Define Actions (Layer 3/4 Policy Map), on page 298.
Step 4

Determine on which interfaces you want to apply the policy map, or apply it globally, as described in Apply Actions to an Interface (Service Policy), on page 300.

Identify Traffic (Layer 3/4 Class Maps)

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. You can create multiple Layer 3/4 class maps for each Layer 3/4 policy map.

Create a Layer 3/4 Class Map for Through Traffic

A Layer 3/4 class map matches traffic based on protocols, ports, IP addresses and other Layer 3 or 4 attributes.

Tip

We suggest that you only inspect traffic on ports on which you expect application traffic; if you inspect all traffic, for example using match any, the ASA performance can be impacted.

Procedure

Step 1

Create a Layer 3/4 class map: class-map class_map_name

Where class_map_name is a string 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. The CLI enters class-map configuration mode.

**Example:**

```
hostname(config)# class-map all_udp
```

**Step 2**

(Optional) Add a description to the class map.

```
description string
```

**Example:**

```
hostname(config-cmap)# description All UDP traffic
```

**Step 3**

Match traffic using one of the following commands. Unless otherwise specified, you can include only one `match` command in the class map.

- **match any**—Matches all traffic.
  ```
  hostname(config-cmap)# match any
  ```

- **match access-list access_list_name**—Matches traffic specified by an extended ACL.
  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port {tcp | udp | sctp} {eq port_num | range port_num port_num}**—Matches destination ports, either a single port or a contiguous range of ports, for the indicated protocol. For applications that use multiple, non-contiguous ports, use the `match access-list` command and define an ACE to match each port.
  ```
  hostname(config-cmap)# match tcp eq 80
  ```

- **match default-inspection-traffic**—Matches default traffic for inspection: the default TCP and UDP ports used by all applications that the ASA can inspect.
  ```
  hostname(config-cmap)# match default-inspection-traffic
  ```

This command, which is used in the default global policy, is a special CLI shortcut that when used in a policy map, 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 ASA, then the ASA applies the TFTP inspection; when TCP traffic for port 21 arrives, then the ASA applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map (with the exception of WAAS inspection, which can be configured with other inspections. See Incompatibility of Certain Feature Actions, on page 288 for more information about combining actions). Normally, the ASA 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 Default Inspections and NAT Limitations, on page 311 for a list of default ports. Not all applications whose ports are included in the `match default-inspection-traffic` command are enabled by default in the policy map.
You can specify a **match access-list** command along with the **match default-inspection-traffic** command to narrow the matched traffic. Because the **match default-inspection-traffic** command specifies the ports and protocols to match, any ports and protocols in the ACL are ignored.

- **match dscp value1 [value2] […] [value8]**—Matches the DSCP value in an IP header, up to eight DSCP values.

  hostname(config-cmap)# match dscp af43 cs1 ef

- **match precedence value1 [value2] [value3] [value4]**—Matches up to four precedence values, represented by the TOS byte in the IP header, where the precedence values can be 0 to 7.

  hostname(config-cmap)# match precedence 1 4

- **match rtp starting_port range**—Matches RTP traffic, where the **starting_port** specifies an even-numbered UDP destination port between 2000 and 65534. The **range** specifies the number of additional UDP ports to match above the **starting_port**, between 0 and 16383.

  hostname(config-cmap)# match rtp 4004 100

- **match tunnel-group name**—Matches VPN tunnel group traffic to which you want to apply QoS.

You can also specify one other **match** command to refine the traffic match. You can specify any of the preceding commands, except for the **match any**, **match access-list**, or **match default-inspection-traffic** commands. Or you can also enter the **match flow ip destination-address** command to match flows in the tunnel group going to each IP address.

  hostname(config-cmap)# match tunnel-group group1
  hostname(config-cmap)# match flow ip destination-address

---

**Examples**

The following is an example for the **class-map** command:

hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http
Create a Layer 3/4 Class Map for Management Traffic

For management traffic to the ASA, you might want to perform actions specific to this kind of traffic. You can specify a management class map that can match an ACL or TCP or UDP ports. The types of actions available for a management class map in the policy map are specialized for management traffic.

Procedure

Step 1
Create a management class map:
```
class-map type management class_map_name
```

Where `class_map_name` is a string 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. The CLI enters class-map configuration mode.

Example:
```
hostname(config)# class-map management all_udp
```

Step 2
(Optional) Add a description to the class map.
```
description string
```

Example:
```
hostname(config-cmap)# description All UDP traffic
```

Step 3
Match traffic using one of the following commands.

- `match access-list access_list_name`—Matches traffic specified by an extended ACL.

  ```
  hostname(config-cmap)# match access-list udp
  ```

- `match port \{tcp | udp | sctp\} \{eq port_num | range port_num port_num\}`—Matches destination ports, either a single port or a contiguous range of ports, for the indicated protocol. For applications that use multiple, non-contiguous ports, use the `match access-list` command and define an ACE to match each port.

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

Define Actions (Layer 3/4 Policy Map)

After you configure Layer 3/4 class maps to identify traffic, use a Layer 3/4 policy map to associate actions to those classes.
Procedure

Step 1  Add the policy map: policy-map policy_map_name

Where policy_map_name is the name of the policy map, up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map. The CLI enters policy-map configuration mode.

Example:

hostname(config)# policy-map global_policy

Step 2  Specify a previously configured Layer 3/4 class map: class class_map_name

Where the class_map_name is the name of the class map.

See Identify Traffic (Layer 3/4 Class Maps), on page 295 to add a class map.

Example:

hostname(config-pmap)# class all_http

Step 3  Specify one or more actions for this class map.

See Features Configured with Service Policies, on page 285.

Note  If there is no match default-inspection-traffic command in a class map, then at most one inspect command is allowed to be configured under the class.

Step 4  Repeat the process for each class map you want to include in this policy map.

Examples

The following is an example of a policy-map command for a connection policy. It limits the number of connections allowed to the web server 10.1.1.1:

hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256

The following example shows how multi-match works in a policy map:
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80
hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000

When a Telnet connection is initiated, it matches class telnet_traffic. Similarly, if an FTP connection is initiated, it matches class ftp_traffic. For any TCP connection other than Telnet and FTP, it will match class tcp_traffic. Even though a Telnet or FTP connection can match class tcp_traffic, the ASA does not make this match because they previously matched other classes.

Apply Actions to an Interface (Service Policy)

To activate the Layer 3/4 policy map, create a service policy that applies it to one or more interfaces or that applies it globally to all interfaces. Use the following command:

```
service-policy policy_map_name {global | interface interface_name} [fail-close]
```

Where:

- `policy_map_name` is the name of the policy map.
- `global` creates a service policy that applies to all interfaces that do not have a specific policy.

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. By default, the configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. The default service policy includes the following command: `service-policy global_policy global`. 
• `interface interface_name` creates a service policy by associating a policy map with an interface.

• `fail-close` generates a syslog (767001) for IPv6 traffic that is dropped by application inspections that do not support IPv6 traffic. By default, syslogs are not generated.

Examples

For example, the following command enables the `inbound_policy` policy map on the outside interface:

```
hostname(config)# service-policy inbound_policy interface outside
```

The following commands disable the default global policy, and enables a new one called `new_global_policy`.

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

Monitoring Service Policies

To monitor service policies, enter the following command:

• `show service-policy`

Displays the service policy statistics.

Examples for Service Policies (Modular Policy Framework)

This section includes several Modular Policy Framework examples.

Applying Inspection and QoS Policing to HTTP Traffic

In this example, any HTTP connection (TCP traffic on port 80) that enters or exits the ASA through the outside interface is classified for HTTP inspection. Any HTTP traffic that exits the outside interface is classified for policing.

*Figure 47: HTTP Inspection and QoS Policing*

See the following commands for this example:
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside

Applying Inspection to HTTP Traffic Globally

In this example, any HTTP connection (TCP traffic on port 80) that enters the ASA through any interface is classified for HTTP inspection. Because the policy is a global policy, inspection occurs only as the traffic enters each interface.

Figure 48: Global HTTP Inspection

See the following commands for this example:

hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy global

Applying Inspection and Connection Limits to HTTP Traffic to Specific Servers

In this example, any HTTP connection destined for Server A (TCP traffic on port 80) that enters the ASA through the outside interface is classified for HTTP inspection and maximum connection limits. Connections initiated from Server A to Host A do not match the ACL in the class map, so they are not affected.

Any HTTP connection destined for Server B that enters the ASA through the inside interface is classified for HTTP inspection. Connections initiated from Server B to Host B do not match the ACL in the class map, so they are not affected.
See the following commands for this example:

```text
hostname(config)# object network obj-192.168.1.2  
hostname(config-network-object)# host 192.168.1.2  
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1  
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0  
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2  
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80  
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80  
hostname(config)# class-map http_serverA  
hostname(config-cmap)# match access-list serverA  
hostname(config)# class-map http_serverB  
hostname(config-cmap)# match access-list serverB  
hostname(config)# policy-map policy_serverA  
hostname(config-pmap)# class http_serverA  
hostname(config-pmap-c)# inspect http  
hostname(config-pmap-c)# set connection conn-max 100  
hostname(config)# policy-map policy_serverB  
hostname(config-pmap)# class http_serverB  
hostname(config-pmap-c)# inspect http  
hostname(config)# service-policy policy_serverB interface inside  
hostname(config)# service-policy policy_serverA interface outside
```

### Applying Inspection to HTTP Traffic with NAT

In this example, the Host on the inside network has two addresses: one is the real IP address 192.168.1.1, and the other is a mapped IP address used on the outside network, 209.165.200.225. You must use the real IP address in the ACL in the class map. If you applied it to the outside interface, you would also use the real address.
See the following commands for this example:

```plaintext
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1, outside) static 209.165.200.225
hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80
hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client
hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_client interface inside
```

### History for Service Policies

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular Policy Framework</td>
<td>7.0(1)</td>
<td>Modular Policy Framework was introduced.</td>
</tr>
<tr>
<td>Management class map for use with RADIUS accounting traffic</td>
<td>7.2(1)</td>
<td>The management class map was introduced for use with RADIUS accounting traffic. The following commands were introduced: class-map type management, and inspect radius-accounting.</td>
</tr>
<tr>
<td>Inspection policy maps</td>
<td>7.2(1)</td>
<td>The inspection policy map was introduced. The following command was introduced: class-map type inspect.</td>
</tr>
<tr>
<td>Regular expressions and policy maps</td>
<td>7.2(1)</td>
<td>Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: class-map type regex, regex, match regex.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Match any for inspection policy maps</td>
<td>8.0(2)</td>
<td>The <strong>match any</strong> keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only <strong>match all</strong> was available.</td>
</tr>
</tbody>
</table>
Getting Started with Application Layer Protocol Inspection

The following topics describe how to configure application layer protocol inspection.

- Application Layer Protocol Inspection, on page 307
- Configure Application Layer Protocol Inspection, on page 315
- Configure Regular Expressions, on page 322
- Monitoring Inspection Policies, on page 325
- History for Application Inspection, on page 327

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 ASA 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 ASA by default, but you might need to enable others depending on your network.

The following topics explain application inspection in more detail.

When to Use Application Protocol Inspection

When a user establishes a connection, the ASA checks the packet against ACLs, 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 ASA.

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 ASA 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 ASA monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

## Inspection Policy Maps

You can configure special actions for many application inspections using an *inspection policy map*. These maps are optional: you can enable inspection for a protocol that supports inspection policy maps without configuring a map. These maps are needed only if you want something other than the default inspection actions.

An inspection policy map consists of one or more of the following elements. The exact options available for an inspection policy map depends on the application.

- **Traffic matching criteria**—You match application traffic to criteria specific to the application, such as a URL string, for which you then enable actions.

  For some traffic matching criteria, you use regular expressions to match text inside a packet. Be sure to create and test the regular expressions before you configure the policy map, either singly or grouped together in a regular expression class map.

- **Inspection class map**—Some inspection policy maps let you use an inspection class map to include multiple traffic matching criteria. You then identify the inspection class map in the inspection policy map and enable actions for the class as a whole. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that you can create more complex match criteria and you can reuse class maps. However, you cannot set different actions for different matches.

- **Parameters**—Parameters affect the behavior of the inspection engine.

The following topics provide more details.

### Replacing an In-Use Inspection Policy Map

If you have an inspection enabled with a policy map in a service policy, replacing the policy map is a two-step process. First, you must remove the inspection. Then, you add it back with the new policy map name.

For example, to replace sip-map1 with sip-map2 in SIP inspection, use the following command sequence:

```bash
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

### How Multiple Traffic Classes are Handled

You can specify multiple inspection class maps or direct matches in the inspection policy map.

If a packet matches multiple different classes or direct matches, then the order in which the ASA applies the actions is determined by internal ASA rules, and not by the order they are added to the inspection policy map. The internal rules are determined by the application type and the logical progression of parsing a packet, and are not user-configurable. For example for HTTP traffic, parsing a Request Method field preceded parsing the Header Host Length field; an action for the Request Method field occurs before the action for the Header Host Length field. For example, the following match commands can be entered in any order, but the `match request method get` command is matched first.
If an action drops a packet, then no further actions are performed in the inspection policy map. For example, if the first action is to reset the connection, then it will never match any further match criteria. If the first action is to log the packet, then a second action, such as resetting the connection, can occur.

If a packet matches multiple match criteria that are the same, then they are matched in the order they appear in the policy map. For example, for a packet with the header length of 1001, it will match the first command below, and be logged, and then will match the second command and be reset. If you reverse the order of the two \texttt{match} commands, then the packet will be dropped and the connection reset before it can match the second \texttt{match} command; it will never be logged.

A class map is determined to be the same type as another class map or direct match based on the lowest priority match option in the class map (the priority is based on the internal rules). If a class map has the same type of lowest priority match option as another class map, then the class maps are matched according to the order they are added to the policy map. If the lowest priority match for each class map is different, then the class map with the higher priority match option is matched first. For example, the following three class maps contain two types of \texttt{match} commands: \texttt{match request-cmd} (higher priority) and \texttt{match filename} (lower priority). The ftp3 class map includes both commands, but it is ranked according to the lowest priority command, \texttt{match filename}. The ftp1 class map includes the highest priority command, so it is matched first, regardless of the order in the policy map. The ftp3 class map is ranked as being of the same priority as the ftp2 class map, which also contains the \texttt{match filename} command. They are matched according to the order in the policy map: ftp3 and then ftp2.

\begin{verbatim}
class-map type inspect ftp match-all ftp1
  match request-cmd get

class-map type inspect ftp match-all ftp2
  match filename regex abc

class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
\end{verbatim}

\section*{Guidelines for Application Inspection}

\subsection*{Failover}

State information for multimedia sessions that require inspection are not passed over the state link for stateful failover. The exceptions are GTP, M3UA, and SIP, which are replicated over the state link. You must configure strict application server process (ASP) state checking in M3UA inspection to get stateful failover.
Clustering

The following inspections are not supported in clustering:

- CTIQBE
- H323, H225, and RAS
- IPsec passthrough
- MGCP
- MMP
- RTSP
- SCCP (Skinny)
- WAAS

IPv6

Supports IPv6 for the following inspections:

- Diameter
- DNS over UDP
- FTP
- GTP
- HTTP
- ICMP
- IPsec pass-through
- IPv6
- M3UA
- SCCP (Skinny)
- SCTP
- SIP
- SMTP
- VXLAN

Supports NAT64 for the following inspections:

- DNS over UDP
- FTP
- HTTP
- ICMP
• SCTP

Additional Guidelines

• Some inspection engines do not support PAT, NAT, outside NAT, or NAT between same security interfaces. For more information about NAT support, see Default Inspections and NAT Limitations, on page 311.

• For all the application inspections, the ASA limits the number of simultaneous, active data connections to 200 connections. For example, if an FTP client opens multiple secondary connections, the FTP inspection engine allows only 200 active connections and the 201 connection is dropped and the adaptive security appliance generates a system error message.

• Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.

• If the system determines that a TCP connection requires inspection, the system clears all TCP options except for the MSS and selective-acknowledgment (SACK) options on the packets before inspecting them. Other options are cleared even if you allow them in a TCP map applied to the connections.

• TCP/UDP Traffic directed to the ASA (to an interface) is inspected by default. However, ICMP traffic directed to an interface is never inspected, even if you enable ICMP inspection. Thus, a ping (echo request) to an interface can fail under specific circumstances, such as when the echo request comes from a source that the ASA can reach through a backup default route.

Defaults for Application Inspection

The following topics explain the default operations for application inspection.

Default Inspections and NAT Limitations

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.

The following table 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. In this table:

• Inspection engines that are enabled by default for the default port are in bold.

• The ASA is in compliance with the indicated 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 ASA does not enforce the order.
Table 12: Supported Application Inspection Engines

<table>
<thead>
<tr>
<th>Application</th>
<th>Default Protocol, Port</th>
<th>NAT Limitations</th>
<th>Standards</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTIQBE</td>
<td>TCP/2748</td>
<td>No extended PAT. No NAT64. (Clustering) No static PAT.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>DCERPC</td>
<td>TCP/135</td>
<td>No NAT64.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Diameter</td>
<td>TCP/3868</td>
<td>No NAT/PAT.</td>
<td>RFC 6733</td>
<td>Requires the Carrier license.</td>
</tr>
<tr>
<td></td>
<td>TCP/5868 (for TCP/TLS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCTP/3868</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS over UDP</td>
<td>UDP/53</td>
<td>No NAT support is available for name resolution through WINS.</td>
<td>RFC 1123</td>
<td>You must enable DNS/TCP inspection in the DNS inspection policy map to inspect DNS over TCP. UDP/443 is used for Cisco Umbrella DNScrypt sessions only.</td>
</tr>
<tr>
<td>DNS over TCP</td>
<td>UDP/443</td>
<td></td>
<td>RFC 959</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP/53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>TCP/21</td>
<td>(Clustering) No static PAT.</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>GTP</td>
<td>UDP/3386 (GTPv0)</td>
<td>No extended PAT. No NAT.</td>
<td>—</td>
<td>Requires the Carrier license.</td>
</tr>
<tr>
<td></td>
<td>UDP/2123 (GTPv1+)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 H.225 and RAS</td>
<td>TCP/1720</td>
<td>(Clustering) No static PAT.</td>
<td>ITU-T H.323, H.245, H225.0, Q.931, Q.932</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>UDP/1718 UDP (RAS) 1718-1719</td>
<td>No extended PAT. No NAT on same security interfaces. No NAT64.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP/80</td>
<td>—</td>
<td>RFC 2616</td>
<td>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.</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP</td>
<td>—</td>
<td>—</td>
<td>ICMP traffic directed to an ASA interface is never inspected.</td>
</tr>
<tr>
<td>ICMP ERROR</td>
<td>ICMP</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>ILS (LDAP)</td>
<td>TCP/389</td>
<td>No extended PAT. No NAT64.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Application</td>
<td>Default Protocol, Port</td>
<td>NAT Limitations</td>
<td>Standards</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Instant Messaging (IM)</td>
<td>Varies by client</td>
<td>No extended PAT.</td>
<td>RFC 3860</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Options</td>
<td>RSVP</td>
<td>No NAT64.</td>
<td>RFC 791, RFC 2113</td>
<td></td>
</tr>
<tr>
<td>IPsec Pass Through</td>
<td>UDP/500</td>
<td>No PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>—</td>
<td>No NAT64.</td>
<td>RFC 2460</td>
<td></td>
</tr>
<tr>
<td>LISP</td>
<td>—</td>
<td>No NAT or PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M3UA</td>
<td>SCTP/2905</td>
<td>No NAT or PAT for embedded addresses.</td>
<td>RFC 4666</td>
<td>Requires the Carrier license.</td>
</tr>
<tr>
<td>MGCP</td>
<td>UDP/2427, 2727</td>
<td>No extended PAT.</td>
<td>RFC 2705bis-05</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Clustering) No static PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMP</td>
<td>TCP/5443</td>
<td>No extended PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS Name Server over IP</td>
<td>UDP/137, 138 (Source ports)</td>
<td>No extended PAT.</td>
<td>RFC 2637</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Clustering) No static PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPTP</td>
<td>TCP/1723</td>
<td>No NAT64.</td>
<td>RFC 2865</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Clustering) No static PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>UDP/1646</td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSH</td>
<td>TCP/514</td>
<td>No PAT.</td>
<td>Berkeley UNIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Clustering) No static PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTSP</td>
<td>TCP/554</td>
<td>No extended PAT.</td>
<td>RFC 2326, 2327, 1889</td>
<td>No handling for HTTP cloaking.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No NAT64.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Clustering) No static PAT.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ScanSafe (Cloud Web Security)</td>
<td>TCP/80 TCP/443</td>
<td>—</td>
<td></td>
<td>These ports are not included in the default-inspection-traffic class for the ScanSafe inspection.</td>
</tr>
<tr>
<td>Application</td>
<td>Default Protocol, Port</td>
<td>NAT Limitations</td>
<td>Standards</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>SCTP</td>
<td>SCTP</td>
<td>—</td>
<td>RFC 4960</td>
<td>Requires the Carrier license. Although you can do static network object NAT on SCTP traffic (no dynamic NAT/PAT), the inspection engine is not used for NAT.</td>
</tr>
<tr>
<td>SIP</td>
<td>TCP/5060, UDP/5060</td>
<td>No NAT/PAT on interfaces with the same, or lower to higher, security levels. No extended PAT. No NAT64 or NAT46. (Clustering) No static PAT.</td>
<td>RFC 2543</td>
<td>Does not handle TFTP uploaded Cisco IP Phone configurations under certain circumstances.</td>
</tr>
<tr>
<td>SKINNY (SCCP)</td>
<td>TCP/2000</td>
<td>No NAT on same security interfaces. No extended PAT. No NAT64, NAT46, or NAT66. (Clustering) No static PAT.</td>
<td>—</td>
<td>Does not handle TFTP uploaded Cisco IP Phone configurations under certain circumstances.</td>
</tr>
<tr>
<td>SMTP and ESMTP</td>
<td>TCP/25</td>
<td>No NAT64.</td>
<td>RFC 821, 1123</td>
<td>—</td>
</tr>
<tr>
<td>SNMP</td>
<td>UDP/161, 162</td>
<td>No NAT or PAT.</td>
<td>RFC 1155, 1157, 1212, 1213, 1215 v.2 RFC 1902-1908; v.3 RFC 2570-2580.</td>
<td>—</td>
</tr>
<tr>
<td>SQL*Net</td>
<td>TCP/1521</td>
<td>No extended PAT. No NAT64. (Clustering) No static PAT.</td>
<td>—</td>
<td>v.1 and v.2.</td>
</tr>
<tr>
<td>STUN</td>
<td>TCP/3478, UDP/3478</td>
<td>(WebRTC) Static NAT/PAT44 only. (Cisco Spark) Static NAT/PAT44 and 64; and dynamic NAT/PAT.</td>
<td>RFC 5245, 5389</td>
<td>—</td>
</tr>
<tr>
<td>Sun RPC</td>
<td>TCP/111, UDP/111</td>
<td>No extended PAT. No NAT64.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>TFTP</td>
<td>UDP/69</td>
<td>No NAT64. (Clustering) No static PAT.</td>
<td>RFC 1350</td>
<td>Payload IP addresses are not translated.</td>
</tr>
<tr>
<td>WAAS</td>
<td>TCP/1-65535</td>
<td>No extended PAT. No NAT64.</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
The default policy configuration includes the following commands:

```
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
  message-length maximum client auto
  message-length maximum 512
  dns-guard
  protocol-enforcement
  nat-rewrite
policy-map global_policy
  class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

**Default Inspection Policy Maps**

Some inspection types use hidden default policy maps. For example, if you enable ESMTP inspection without specifying a map, _default_esmtp_map is used.

The default inspection is described in the sections that explain each inspection type. You can view these default maps using the `show running-config all policy-map` command.

DNS inspection is the only one that uses an explicitly-configured default map, preset_dns_map.

**Configure Application Layer Protocol Inspection**

You configure application inspection in service policies.

Inspection is enabled by default globally on all interfaces for some applications on their standard ports and protocols. See Default Inspections and NAT Limitations, on page 311 for more information on default...
inspections. A common method for customizing the inspection configuration is to customize the default global policy. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

**Before you begin**

For some applications, you can perform special actions when you enable inspection by configuring inspection policy maps. The table later in this procedure shows which protocols allow inspection policy maps, with pointers to the instructions on configuring them. If you want to configure these advanced features, create the map before configuring inspection.

**Procedure**

**Step 1**

Unless you are adding inspection to an existing class map, create an L3/L4 class map to identify the traffic for which you want to apply the inspection.

```
class-map name
match parameter
```

**Example:**

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

In the default global policy, the inspection_default class map is a special class map that includes default ports for all inspection types (*match default-inspection-traffic*). You can have more than one inspection on the inspection_default class only, and you might want to simply edit the existing global policy that applies the inspection defaults. If you are using this class map in either the default policy or for a new service policy, you can skip this step. For detailed information on which class map to choose, see Choosing the Right Traffic Class for Inspection, on page 321.

For information on matching statements, see Create a Layer 3/4 Class Map for Through Traffic, on page 295. For RADIUS accounting inspection, which uses a management layer 3/4 class, see Configure RADIUS Accounting Inspection, on page 427.

**Step 2**

Add or edit a Layer 3/4 policy map that sets the actions to take with the class map traffic: `policy-map name`

**Example:**

```
hostname(config)# policy-map global_policy
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name.

**Step 3**

Identify the L3/L4 class map you are using for inspection: `class name`

**Example:**

```
hostname(config-pmap)# class inspection_default
```

To edit the default policy, or to use the special inspection_default class map in a new policy, specify `inspection_default` for the `name`. Otherwise, you are specifying the class you created earlier in this procedure.
You can combine multiple class maps in the same policy if desired, so you can create one class map to match certain traffic, and another to match different traffic. However, if traffic matches a class map that contains an inspection command, and then matches another class map that also has an inspection command, only the first matching class is used. For example, SNMP matches the inspection_default class map. To enable SNMP inspection, enable SNMP inspection for the default class. Do not add another class that matches SNMP.

**Step 4**

Enable application inspection: `inspect protocol`

The `protocol` is one of the following values:

**Table 13: Inspection Protocol Keywords**

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ctiqbe</code></td>
<td>See CTIQBE Inspection, on page 369.</td>
</tr>
<tr>
<td><code>dcerpc [map_name]</code></td>
<td>See DCERPC Inspection, on page 329.</td>
</tr>
<tr>
<td></td>
<td>If you added a DCERPC inspection policy map according to Configure a DCERPC Inspection Policy Map, on page 330, identify the map name in this command.</td>
</tr>
<tr>
<td><code>diameter [map_name] [tls-proxy proxy_name]</code></td>
<td>See Diameter Inspection, on page 397.</td>
</tr>
<tr>
<td></td>
<td>If you added a Diameter inspection policy map according to Configure a Diameter Inspection Policy Map, on page 406, identify the map name in this command.</td>
</tr>
<tr>
<td></td>
<td><code>tls-proxy proxy_name</code> identifies the TLS proxy to use for this inspection. You need a TLS proxy only if you want to enable inspection of encrypted traffic.</td>
</tr>
<tr>
<td><code>dns [map_name] [dynamic-filter-snoop]</code></td>
<td>See DNS Inspection, on page 332.</td>
</tr>
<tr>
<td></td>
<td>If you added a DNS inspection policy map according to Configure DNS Inspection Policy Map, on page 333, identify the map name in this command. The default DNS inspection policy map name is “preset_dns_map.”</td>
</tr>
<tr>
<td></td>
<td><code>dynamic-filter-snoop</code> enables dynamic filter snooping, which is used exclusively by the Botnet Traffic Filter. Include this keyword only if you use Botnet Traffic Filtering. We suggest that you enable DNS snooping only on interfaces where external DNS requests are going. Enabling DNS snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the ASA.</td>
</tr>
<tr>
<td><code>esmtp [map_name]</code></td>
<td>See SMTP and Extended SMTP Inspection, on page 357.</td>
</tr>
<tr>
<td></td>
<td>If you added an ESMTP inspection policy map according to Configure an ESMTP Inspection Policy Map, on page 359, identify the map name in this command.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ftp [strict [map_name]]</td>
<td>See FTP Inspection, on page 337. Use the <strong>strict</strong> keyword to increase the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. See Strict FTP, on page 337 for more information. If you added an FTP inspection policy map according to Configure an FTP Inspection Policy Map, on page 338, identify the map name in this command.</td>
</tr>
<tr>
<td>gtp [map_name]</td>
<td>See GTP Inspection Overview, on page 393. If you added a GTP inspection policy map according to Configure a GTP Inspection Policy Map, on page 401, identify the map name in this command.</td>
</tr>
<tr>
<td>h323 h225 [map_name]</td>
<td>See H.323 Inspection, on page 370. If you added an H323 inspection policy map according to Configure H.323 Inspection Policy Map, on page 372, identify the map name in this command.</td>
</tr>
<tr>
<td>h323 ras [map_name]</td>
<td>See H.323 Inspection, on page 370. If you added an H323 inspection policy map according to Configure H.323 Inspection Policy Map, on page 372, identify the map name in this command.</td>
</tr>
<tr>
<td>http [map_name]</td>
<td>See HTTP Inspection, on page 341. If you added an HTTP inspection policy map according to Configure an HTTP Inspection Policy Map, on page 342, identify the map name in this command.</td>
</tr>
<tr>
<td>icmp</td>
<td>See ICMP Inspection, on page 346.</td>
</tr>
<tr>
<td>icmp error</td>
<td>See ICMP Error Inspection, on page 346.</td>
</tr>
<tr>
<td>ils</td>
<td>See ILS Inspection, on page 347.</td>
</tr>
<tr>
<td>im [map_name]</td>
<td>See Instant Messaging Inspection, on page 347. If you added an Instant Messaging inspection policy map, identify the map name in this command.</td>
</tr>
<tr>
<td>ip-options [map_name]</td>
<td>See IP Options Inspection, on page 350. If you added an IP Options inspection policy map according to Configure an IP Options Inspection Policy Map, on page 351, identify the map name in this command.</td>
</tr>
<tr>
<td>ipsec-pass-thru [map_name]</td>
<td>See IPsec Pass Through Inspection, on page 352. If you added an IPsec Pass Through inspection policy map according to Configure an IPsec Pass Through Inspection Policy Map, on page 353, identify the map name in this command.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
</tr>
<tr>
<td>ipv6 [map_name]</td>
<td>See IPv6 Inspection, on page 354. If you added an IPv6 inspection policy map according to Configure an IPv6 Inspection Policy Map, on page 354, identify the map name in this command.</td>
</tr>
<tr>
<td>lisp [map_name]</td>
<td>For detailed information on configuring LISP, including inspection, see the clustering chapter in the general configuration guide. If you added a LISP inspection policy map, identify the map name in this command.</td>
</tr>
<tr>
<td>m3ua [map_name]</td>
<td>See M3UA Inspection, on page 397. If you added an M3UA inspection policy map according to Configure an M3UA Inspection Policy Map, on page 422, identify the map name in this command.</td>
</tr>
<tr>
<td>mgcp [map_name]</td>
<td>See MGCP Inspection, on page 375. If you added an MGCP inspection policy map according to Configure an MGCP Inspection Policy Map, on page 376, identify the map name in this command.</td>
</tr>
<tr>
<td>netbios [map_name]</td>
<td>See NetBIOS Inspection, on page 356. If you added a NetBIOS inspection policy map, identify the map name in this command.</td>
</tr>
<tr>
<td>pptp</td>
<td>See PPTP Inspection, on page 357.</td>
</tr>
<tr>
<td>radius-accounting</td>
<td>See RADIUS Accounting Inspection Overview, on page 399. The radius-accounting keyword is only available for a management class map. You must specify a RADIUS accounting inspection policy map; see Configure a RADIUS Accounting Inspection Policy Map, on page 427.</td>
</tr>
<tr>
<td>rsh</td>
<td>See RSH Inspection, on page 357.</td>
</tr>
<tr>
<td>rtsp [map_name]</td>
<td>See RTSP Inspection, on page 378. If you added a RTSP inspection policy map according to Configure RTSP Inspection Policy Map, on page 379, identify the map name in this command.</td>
</tr>
<tr>
<td>scansafe [map_name] [fail-open</td>
<td>fail-closed]</td>
</tr>
</tbody>
</table>
### Configure Application Layer Protocol Inspection

**Keywords** | **Notes**
--- | ---
`sctp [map_name]` | See SCTP Application Layer Inspection, on page 396. If you added an SCTP inspection policy map according to Configure an SCTP Inspection Policy Map, on page 405, identify the map name in this command.

**sip [map_name] [tls-proxy proxy_name]** | See SIP Inspection, on page 381. If you added a SIP inspection policy map according to Configure SIP Inspection Policy Map, on page 383, identify the map name in this command. **tls-proxy proxy_name** identifies the TLS proxy to use for this inspection. You need a TLS proxy only if you want to enable inspection of encrypted traffic.

**skinny [map_name] [tls-proxy proxy_name]** | See Skinny (SCCP) Inspection, on page 386. If you added a Skinny inspection policy map according to Configure a Skinny (SCCP) Inspection Policy Map, on page 388, identify the map name in this command. **tls-proxy proxy_name** identifies the TLS proxy to use for this inspection. You need a TLS proxy only if you want to enable inspection of encrypted traffic.

**snmp [map_name]** | See SNMP Inspection, on page 362. If you added an SNMP inspection policy map, identify the map name in this command.

**sqlnet** | See SQL*Net Inspection, on page 363.

**stun** | See STUN Inspection, on page 389.

**sunrpc** | See Sun RPC Inspection, on page 363. The default class map includes UDP port 111; if you want to enable Sun RPC inspection for TCP port 111, you need to create a new class map that matches TCP port 111, add the class to the policy, and then apply the `inspect sunrpc` command to that class.

**tftp** | See TFTP Inspection, on page 364.

**waas** | Enables TCP option 33 parsing. Use when deploying Cisco Wide Area Application Services products.

**xdmcp** | See XDMCP Inspection, on page 365.

**vxlan** | See VXLAN Inspection, on page 365.

### Note
If you are editing the default global policy (or any in-use policy) to use a different inspection policy map, you must remove the old inspection with the `no inspect protocol` command, and then re-add it with the new inspection policy map name.
Choosing the Right Traffic Class for Inspection

The default Layer 3/4 class map for through traffic is called “inspection_default.” It matches traffic using a special match command, match default-inspection-traffic, to match the default protocols and ports for each application protocol. This traffic class (along with match any, which is not typically used for inspection) matches both IPv4 and IPv6 traffic for inspections that support IPv6. See Guidelines for Application Inspection, on page 309 for a list of IPv6-enabled inspections.

You can specify a match access-list command along with the match default-inspection-traffic command to narrow the matched traffic to specific IP addresses. Because the match default-inspection-traffic command specifies the ports to match, any ports in the ACL are ignored.

Tip

We suggest that you only inspect traffic on ports on which you expect application traffic; if you inspect all traffic, for example using match any, the ASA performance can be impacted.

If you want to match non-standard ports, then create a new class map for the non-standard ports. See Default Inspections and NAT Limitations, on page 311 for the standard ports for each inspection engine. You can combine multiple class maps in the same policy if desired, so you can create one class map to match certain traffic, and another to match different traffic. However, if traffic matches a class map that contains an inspection command, and then matches another class map that also has an inspection command, only the first matching class is used. For example, SNMP matches the inspection_default class. To enable SNMP inspection, enable SNMP inspection for the default class. Do not add another class that matches SNMP.

For example, to limit inspection to traffic from 10.1.1.0 to 192.168.1.0 using the default class map, enter the following commands:

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

View the entire class map using the following command:
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
  match default-inspection-traffic
    match access-list inspect
!
To inspect FTP traffic on port 21 as well as 1056 (a non-standard port), create an ACL that specifies the ports, and assign it to a new class map:

hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect

Configure Regular Expressions

Regular expressions define pattern matching for text strings. You can use these expressions in some protocol inspection maps to match packets based on strings such as URLs or the contents of particular header fields.

Create a Regular Expression

A regular expression matches text strings either literally as an exact string, or by using metacharacters so that 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 a URL string inside an HTTP packet.

Before you begin

Use Ctrl+V to escape all of the special characters in the CLI, such as question mark (?) or a tab. For example, type d[Ctrl+V]?g to enter d?g in the configuration.

See the regex command in the command reference for performance impact information when matching a regular expression to packets. In general, matching against long input strings, or trying to match a large number of regular expressions, will reduce system performance.

Note

As an optimization, the ASA 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.

The following table lists the metacharacters that have special meanings.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Dot</td>
<td>Matches any single character. For example, d,g matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td><code>(exp)</code></td>
<td>Subexpression</td>
<td>A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, `d(o</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
<td>Alternation</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Question mark</td>
<td>A quantifier that indicates that there are 0 or 1 of the previous expression. For example, <code>lo?se</code> matches ise or lose.</td>
</tr>
<tr>
<td><code>*</code></td>
<td>Asterisk</td>
<td>A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, <code>lo*se</code> matches ise, lose, loose, and so on.</td>
</tr>
<tr>
<td><code>+</code></td>
<td>Plus</td>
<td>A quantifier that indicates that there is at least 1 of the previous expression. For example, <code>lo+se</code> matches lose and loose, but not ise.</td>
</tr>
<tr>
<td><code>{x}</code> or <code>{x,}</code></td>
<td>Minimum repeat quantifier</td>
<td>Repeat at least x times. For example, <code>ab(xy){2,}z</code> matches abxyxyz, abxyxyxyz, and so on.</td>
</tr>
<tr>
<td><code>[abc]</code></td>
<td>Character class</td>
<td>Matches any character in the brackets. For example, <code>[abc]</code> matches a, b, or c.</td>
</tr>
<tr>
<td><code>[^abc]</code></td>
<td>Negated character class</td>
<td>Matches a single character that is not contained within the brackets. For example, <code>[^abc]</code> matches any character other than a, b, or c. <code>[^A-Z]</code> matches any single character that is not an uppercase letter.</td>
</tr>
<tr>
<td><code>[a-c]</code></td>
<td>Character range class</td>
<td>Matches any character in the range. <code>[a-z]</code> matches any lowercase letter. You can mix characters and ranges: <code>[abcq-z]</code> matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does <code>[a-cq-z]</code>. The dash (-) character is literal only if it is the last or the first character within the brackets: <code>[abc]-</code> or <code>[-abc]</code>.</td>
</tr>
<tr>
<td><code>&quot;&quot;</code></td>
<td>Quotation marks</td>
<td>Preserves trailing or leading spaces in the string. For example, <code>&quot; test&quot;</code> preserves the leading space when it looks for a match.</td>
</tr>
<tr>
<td><code>^</code></td>
<td>Caret</td>
<td>Specifies the beginning of a line.</td>
</tr>
<tr>
<td><code>\</code></td>
<td>Escape character</td>
<td>When used with a metacharacter, matches a literal character. For example, <code>\</code> matches the left square bracket.</td>
</tr>
</tbody>
</table>
When character is not a metacharacter, matches the literal character.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>char</td>
<td>Character</td>
<td>When character is not a metacharacter, matches the literal character.</td>
</tr>
<tr>
<td>\r</td>
<td>Carriage return</td>
<td>Matches a carriage return 0x0d.</td>
</tr>
<tr>
<td>\n</td>
<td>Newline</td>
<td>Matches a new line 0x0a.</td>
</tr>
<tr>
<td>\t</td>
<td>Tab</td>
<td>Matches a tab 0x09.</td>
</tr>
<tr>
<td>\f</td>
<td>Formfeed</td>
<td>Matches a form feed 0x0c.</td>
</tr>
<tr>
<td>\xNN</td>
<td>Escaped hexadecimal number</td>
<td>Matches an ASCII character using hexadecimal (exactly two digits).</td>
</tr>
<tr>
<td>\NNN</td>
<td>Escaped octal number</td>
<td>Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.</td>
</tr>
</tbody>
</table>

Procedure

### Step 1
Test a regular expression to make sure it matches what you think it will match: **test regex input_text regular_expression**

Where the **input_text** argument is a string you want to match using the regular expression, up to 201 characters in length. The **regular_expression** argument can be up to 100 characters in length.

Use Ctrl+V to escape all of the special characters in the CLI. For example, to enter a tab in the input text in the **test regex** command, you must enter **test regex “test[Ctrl+V Tab]” “test\t”**.

If the regular expression matches the input text, you see the following message:

INFO: Regular expression match succeeded.

If the regular expression does not match the input text, you see the following message:

INFO: Regular expression match failed.

### Step 2
To add a regular expression after you tested it, enter the following command: **regex name regular_expression**

Where the **name** argument can be up to 40 characters in length. The **regular_expression** argument can be up to 100 characters in length.

Examples

The following example creates two regular expressions for use in an inspection policy map:
Create a Regular Expression Class Map

A regular expression class map identifies one or more regular expression. It is simply a collection of regular expression objects. You can use a regular expression class map in many cases in replace of a regular expression object.

Procedure

Step 1  Create the regular expression class map: class-map type regex match-any class_map_name
Where class_map_name is a string 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.

The match-any keyword specifies that the traffic matches the class map if it matches at least one of the regular expressions.

Step 2  (Optional) Add a description to the class map: description string

Step 3  Identify the regular expressions you want to include by entering the following command for each regular expression: match regex regex_name

Examples

The following example creates two regular expressions, and adds them to a regular expression class map. Traffic matches the class map if it includes the string “example.com” or “example2.com.”

hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com

hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2

Monitoring Inspection Policies

To monitor inspection service policies, enter the following commands. See the command reference on Cisco.com for detailed syntax and examples.

• show service-policy inspect protocol

Displays statistics for inspection service policies. The protocol is the protocol from the inspect command, for example dns. However, not all inspection protocols show statistics with this command. For example:

asa# show service-policy inspect dns
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
message-length maximum client auto, drop 0
message-length maximum 512, drop 0
dns-guard, count 0
protocol-enforcement, drop 0
nat-rewrite, count 0
asa#

• **show conn**
  
  Shows current connections for traffic passing through the device. This command has a wide range of keywords so that you can get information about various protocols.

• Additional commands for specific inspected protocols:
  
  • **show ctiqbe**
    
    Displays information about the media connections allocated by the CTIQBE inspection engine
  
  • **show h225**
    
    Displays information for H.225 sessions.
  
  • **show h245**
    
    Displays information for H.245 sessions established by endpoints using slow start.
  
  • **show h323 ras**
    
    Displays connection information for H.323 RAS sessions established between a gatekeeper and its H.323 endpoint.
  
  • **show mgcp {commands | sessions }**
    
    Displays the number of MGCP commands in the command queue or the number of existing MGCP sessions.
  
  • **show sip**
    
    Displays information for SIP sessions.
  
  • **show skinny**
    
    Displays information for Skinny (SCCP) sessions.
  
  • **show sunrpc-server active**
    
    Displays the pinholes opened for Sun RPC services.
### History for Application Inspection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection policy maps</td>
<td>7.2(1)</td>
<td>The inspection policy map was introduced. The following command was introduced: <code>class-map type inspect</code>.</td>
</tr>
<tr>
<td>Regular expressions and policy maps</td>
<td>7.2(1)</td>
<td>Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: <code>class-map type regex</code>, <code>regex</code>, <code>match regex</code>.</td>
</tr>
<tr>
<td>Match any for inspection policy maps</td>
<td>8.0(2)</td>
<td>The <strong>match any</strong> keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only <strong>match all</strong> was available.</td>
</tr>
</tbody>
</table>
Inspection of Basic Internet Protocols

The following topics explain application inspection for basic Internet protocols. For information on why you need to use inspection for certain protocols, and the overall methods for applying inspection, see Getting Started with Application Layer Protocol Inspection, on page 307.

- DCERPC Inspection, on page 329
- DNS Inspection, on page 332
- FTP Inspection, on page 337
- HTTP Inspection, on page 341
- ICMP Inspection, on page 346
- ICMP Error Inspection, on page 346
- ILS Inspection, on page 347
- Instant Messaging Inspection, on page 347
- IP Options Inspection, on page 350
- IPsec Pass Through Inspection, on page 352
- IPv6 Inspection, on page 354
- NetBIOS Inspection, on page 356
- PPTP Inspection, on page 357
- RSH Inspection, on page 357
- SMTP and Extended SMTP Inspection, on page 357
- SNMP Inspection, on page 362
- SQL*Net Inspection, on page 363
- Sun RPC Inspection, on page 363
- TFTP Inspection, on page 364
- XDMCP Inspection, on page 365
- VXLAN Inspection, on page 365
- History for Basic Internet Protocol Inspection, on page 366

DCERPC Inspection

DCERPC inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add DCERPC inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

The following sections describe the DCERPC inspection engine.
DCERPC Overview

Microsoft Remote Procedure Call (MSRPC), based on 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.

The DCERPC inspection engine inspects 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 configurable timeouts.

DCE inspection supports the following universally unique identifiers (UUIDs) and messages:

- Endpoint mapper (EPM) UUID. All EPM messages are supported.
- ISystemMapper UUID (non-EPM). Supported messages are:
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- OxidResolver UUID (non-EPM). Supported message is:
  - ServerAlive2 opnum5
- Any message that does not contain an IP address or port information because these messages do not require inspection.

Configure a DCERPC Inspection Policy Map

To specify additional DCERPC inspection parameters, create a DCERPC inspection policy map. You can then apply the inspection policy map when you enable DCERPC inspection.

When defining traffic matching criteria, you can either create a class map or include the match statements directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that you can reuse class maps.

Procedure

Step 1 (Optional) Create a DCERPC inspection class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a) Create the class map: `class-map type inspect dcerpc [match-all | match-any] class_map_name`
Configure a DCERPC Inspection Policy Map

Where `class_map_name` is the name of the class map. The `match-all` keyword is the default, and specifies that traffic must match all criteria to match the class map. The `match-any` keyword specifies that the traffic matches the class map if it matches at least one `match` statement. The CLI enters class-map configuration mode.

b) Specify the traffic on which you want to perform actions using the following `match` command. If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

- `match [not] uuid type`—Matches the universally unique identifier (UUID) of the DCERPC message. The `type` can be one of the following:
  - `ms-rpc-epm`—Matches Microsoft RPC EPM messages.
  - `ms-rpc-isystemactivator`—Matches ISystemMapper messages.
  - `ms-rpc-oxidresolver`—Matches OxidResolver messages.

c) Enter `exit` to leave class map configuration mode.

**Step 2**
Create a DCERPC inspection policy map: `policy-map type inspect dcerpc policy_map_name`
Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 3**
(Optional) Add a description to the policy map: `description string`

**Step 4**
To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created a DCERPC class map, specify it by entering the following command: `class class_map_name`

- Specify traffic directly in the policy map using one of the `match` commands described for DCERPC class maps. If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

- `reset [log]`—Drop the packet, close the connection, and send a TCP reset to the server or client.
- `log`—Send a system log message. You can use this option alone or with one of the other actions.

You can specify multiple `class` or `match` commands in the policy map.

**Example:**

```plaintext
hostname(config)# policy-map type inspect dcerpc dcerpc-map
hostname(config-pmap)# match uuid ms-rpc-epm
hostname(config-pmap-c)# log
```

**Step 5**
To configure parameters that affect the inspection engine, perform the following steps.

a) Enter parameters configuration mode:

```plaintext
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```
b) Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option:

- **timeout pinhole hh:mm:ss**—Configures the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes. The timeout can be from 00:00:01 to 119:00:00.

- **endpoint-mapper [epm-service-only] [lookup-operation [timeout hh:mm:ss]]**—Configures options for the endpoint mapper traffic. The **epm-service-only** keyword enforces endpoint mapper service during binding so that only its service traffic is processed. The **lookup-operation** keyword enables the lookup operation of the endpoint mapper service. You can configure the timeout for pinholes generated from the lookup operation. If no timeout is configured for the lookup operation, the timeout pinhole command or the default is used.

**Examples**

The following example shows how to define a DCERPC inspection policy map with the timeout configured for DCERPC pinholes.

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

**What to do next**

You can now configure an inspection policy to use the map. See [Configure Application Layer Protocol Inspection](#), on page 315.

**DNS Inspection**

DNS inspection is enabled by default. You need to configure it only if you want non-default processing. The following sections describe DNS application inspection.

**Defaults for DNS Inspection**

DNS inspection is enabled by default, using the preset _dns_map_ inspection class map:

- The maximum DNS message length is 512 bytes.
- DNS over TCP inspection is disabled.
- The maximum client DNS message length is automatically set to match the Resource Record.
• DNS Guard is enabled, so the ASA tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the ASA. The ASA also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

• Translation of the DNS record based on the NAT configuration is enabled.

• Protocol enforcement is enabled, which enables DNS message format check, including domain name length of no more than 255 characters, label length of 63 characters, compression, and looped pointer check.

See the following default DNS inspection commands:

```
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
! ...
service-policy global_policy global
```

Configure DNS Inspection Policy Map

You can create a DNS inspection policy map to customize DNS inspection actions if the default inspection behavior is not sufficient for your network.

**Before you begin**

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

**Procedure**

**Step 1**

(Optional) Create a DNS inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify `match` commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the `match not` command. For example, if the `match not` command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each `match` command, you should identify the traffic directly in the policy map.
Step 2
Create a DNS inspection policy map: `policy-map type inspect dns policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 3
(Optional) Add a description to the policy map: `description string`

Step 4
To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:

   • If you created a DNS class map, specify it by entering the following command: `class class_map_name`
• Specify traffic directly in the policy map using one of the **match** commands described for DNS class maps. If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

- **drop [log]**—Drop all packets that match.
- **drop-connection [log]**—Drop the packet and close the connection.
- **mask [log]**—Mask out the matching portion of the packet. This action is available for header flag matches only.
- **log**—Send a system log message. You can use this option alone or with one of the other actions.
- **enforce-tsig [drop] [log]**—Enforce the presence of the TSIG resource record in a message. You can drop a packet without the TSIG resource record, log it, or drop and log it. You can use this option in conjunction with the mask action for header flag matches; otherwise, this action is exclusive with the other actions.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see How Multiple Traffic Classes are Handled, on page 308.

**Example:**

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

**Step 5**

To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option.

- **dncrypt**—Enables DNSCrypt to encrypt connections between the device and Cisco Umbrella. Enabling DNSCrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key. Because DNSCrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.

- **dns-guard**—Enables DNS Guard. The ASA tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the ASA. The ASA also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

- **id-mismatch count number duration seconds action log**—Enables logging for excessive DNS ID mismatches, where the **count number duration seconds** arguments specify the maximum number of mismatch instances per second before a system message log is sent.

- **id-randomization**—Randomizes the DNS identifier for a DNS query.
Configure DNS Inspection Policy Map

- **message-length maximum** \{length | client \{length | auto\} | server \{length | auto\}\}—Sets the maximum DNS message length, from 512 to 65535 bytes. You can also set the maximum length for client or server messages. The **auto** keyword sets the maximum length to the value in the Resource Record.

- **nat-rewrite**—Translates the DNS record based on the NAT configuration.

- **protocol-enforcement**—Enables DNS message format check, including domain name length of no more than 255 characters, label length of 63 characters, compression, and looped pointer check.

- **tcp-inspection**—Enables inspection of DNS over TCP traffic. Ensure that DNS/TCP port 53 traffic is part of the class to which you apply DNS inspection. The inspection default class includes TCP/53.

- **tsig enforced action** \{[drop] [log]\}—Requires a TSIG resource record to be present. You can **drop** a non-conforming packet, **log** the packet, or both.

- **umbrella** \{tag umbrella_policy\}—Enables Cisco Umbrella and optionally specifies the name of the Cisco Umbrella policy (tag) to apply to the device. If you do not specify a policy, the default policy is applied. For more information, see Cisco Umbrella, on page 149.

**Example:**

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

**Example**

The following example shows a how to use a new inspection policy map in the global default configuration:

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
  match regex domain_example
  match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
  match not header-flag QR
  match question
  match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
  class pub_server_map
    drop log
    match header-flag RD
    mask log
  parameters
    message-length maximum client auto
    message-length maximum 512
```
What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

FTP Inspection

FTP inspection is enabled by default. You need to configure it only if you want non-default processing. The following sections describe the FTP inspection engine.

FTP Inspection Overview

The FTP application inspection inspects the FTP sessions and performs four tasks:

• Prepares dynamic secondary data connection 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.

• Tracks the FTP command-response sequence.

• Generates an audit trail.
  • Audit record 303002 is generated for each file that is retrieved or uploaded.
  • Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

• Translates the embedded IP address.

Note

If you disable FTP inspection, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

Strict FTP

Strict FTP increases the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. To enable strict FTP, include the strict option with the inspect ftp command.

When you use strict FTP, you can optionally specify an FTP inspection policy map to specify FTP commands that are not permitted to pass through the ASA.
Strict FTP inspection enforces the following behavior:

- An FTP command must be acknowledged before the ASA allows a new command.
- The ASA 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 strict FTP may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

With strict FTP inspection, 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 ASA 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 ASA 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 no mask-syst-reply command in the FTP map.

Configure an FTP Inspection Policy Map

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.
If you want FTP inspection to allow FTP servers to reveal their system type to FTP clients, and limit the allowed FTP commands, then create and configure an FTP inspection policy map. You can then apply the map when you enable FTP inspection.

**Before you begin**

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Optional) Create an FTP inspection class map by performing the following steps.</strong></td>
</tr>
</tbody>
</table>

A class map groups multiple traffic matches. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

a) Create the class map: `class-map type inspect ftp [match-all | match-any] class_map_name`

   Where **class_map_name** is the name of the class map. The **match-all** keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one **match** statement. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

b) **(Optional) Add a description to the class map:** `description string`

   Where **string** is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following **match** commands. If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

   - **match [not] filename regex {regex_name | class class_name}**—Matches the filename in the FTP transfer against the specified regular expression or regular expression class.

   - **match [not] filetype regex {regex_name | class class_name}**—Matches the file type in the FTP transfer against the specified regular expression or regular expression class.

   - **match [not] request-command ftp_command [ftp_command...]**—Matches the FTP command, one or more of the following:

     - **APPE**—Append to a file.

     - **CDUP**—Changes to the parent directory of the current working directory.

     - **DELE**—Delete a file on the server.
Configure an FTP Inspection Policy Map

- GET—Gets a file from the server.
- HELP—Provides help information.
- MKD—Makes a directory on the server.
- PUT—Sends a file to the server.
- RMD—Deletes a directory on the server.
- RNFR—Specifies the “rename-from” filename.
- RNTO—Specifies the “rename-to” filename.
- SITE—Used to specify a server-specific command. This is usually used for remote administration.
- STOU—Stores a file using a unique file name.

- match [not] server regex \{regex_name | class class_name\}—Matches the FTP server name against the specified regular expression or regular expression class.

- match [not] username regex \{regex_name | class class_name\}—Matches the FTP username against the specified regular expression or regular expression class.

d) Enter exit to leave class map configuration mode.

Step 2 Create an FTP inspection policy map: policy-map type inspect ftp policy_map_name

Where the policy_map_name is the name of the policy map. The CLI enters policy-map configuration mode.

Step 3 (Optional) Add a description to the policy map: description string

Step 4 To apply actions to matching traffic, perform the following steps:

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created an FTP class map, specify it by entering the following command: class class_map_name

- Specify traffic directly in the policy map using one of the match commands described for FTP class maps. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering the following command:

- reset [log]—Drop the packet, close the connection, and send a TCP reset to the server or client. Add the log keyword to send a system log message.

You can specify multiple class or match commands in the policy map. For information about the order of class and match commands, see How Multiple Traffic Classes are Handled, on page 308.

Step 5 To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode.

hostname(config-pmap)# parameters
hostname(config-pmap-p)#
b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:
   - **mask-banner**—Masks the greeting banner from the FTP server.
   - **mask-syst-reply**—Masks the reply to syst command.

---

**Example**

Before submitting a username and password, all FTP users are presented with a greeting banner. By default, this banner includes version information useful to hackers trying to identify weaknesses in a system. The following example shows how to mask this banner:

```bash
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

**What to do next**

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

---

**HTTP Inspection**

If you are not using a purpose-built module for HTTP inspection and application filtering, such as ASA CX or ASA FirePOWER, you can manually configure HTTP inspection on the ASA.

HTTP inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. However, the default inspect class does include the default HTTP ports, so you can simply edit the default global inspection policy to add HTTP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

---

**Tip**

Do not configure HTTP inspection in both a service module and on the ASA, as the inspections are not compatible.

The following sections describe the HTTP inspection engine.
HTTP Inspection Overview

Tip
You can install a service module that performs application and URL filtering, which includes HTTP inspection, such as ASA CX or ASA FirePOWER. The HTTP inspection running on the ASA is not compatible with these modules. Note that it is far easier to configure application filtering using a purpose-built module rather than trying to manually configure it on the ASA using an HTTP inspection policy map.

Use the HTTP inspection engine to protect against specific attacks and other threats that are associated with HTTP traffic.

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.

The enhanced HTTP inspection feature, which is also known as an application firewall and is available when you configure an HTTP inspection policy map, can help prevent attackers from using HTTP messages for circumventing network security policy.

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.

Enhanced HTTP inspection verifies the following for all HTTP messages:

- Conformance to RFC 2616
- Use of RFC-defined methods only.
- Compliance with the additional criteria.

Configure an HTTP Inspection Policy Map

To specify actions when a message violates a parameter, create an HTTP inspection policy map. You can then apply the inspection policy map when you enable HTTP inspection.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

Procedure

Step 1
(Optional) Create an HTTP inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.
To specify traffic that should not match the class map, use the `match not` command. For example, if the `match not` command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each `match` command, you should identify the traffic directly in the policy map.

a) Create the class map: `class-map type inspect http [match-all | match-any] class_map_name`
   
   Where `class_map_name` is the name of the class map. The `match-all` keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one `match` statement. The CLI enters class-map configuration mode, where you can enter one or more `match` commands.

b) (Optional) Add a description to the class map: `description string`
   
   Where `string` is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following `match` commands.
   
   If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

- `match [not] req-resp content-type mismatch`—Matches traffic with a content-type field in the HTTP response that does not match the accept field in the corresponding HTTP request message.

- `match [not] request args regex {regex_name | class class_name}`—Matches text found in the HTTP request message arguments against the specified regular expression or regular expression class.

- `match [not] request body {regex {regex_name | class class_name} | length gt bytes}`—Matches text found in the HTTP request message body against the specified regular expression or regular expression class, or messages where the request body is greater than the specified length.

- `match [not] request header {field | regex regex_name} regex {regex_name | class class_name}`—Matches the content of a field in the HTTP request message header against the specified regular expression or regular expression class. You can specify the field name explicitly or match the field name to a regular expression. Field names are: 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.

- `match [not] request header {field | regex regex_name} {length gt bytes | count gt number} {length gt bytes | count gt number | non-ascii}`—Matches the length of the specified fields in the HTTP request message header, or the overall number of fields (count) in the header. You can specify the field name explicitly or match the field name to a regular expression or regular expression class. Field names are listed in the previous bullet.

- `match [not] request method {method | regex regex_name} class class_name`—Matches the HTTP request method. You can specify the method explicitly or match the method to a regular
**Configure an HTTP Inspection Policy Map**

Expression or regular expression class. Methods are: 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, relabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.

- **match [not] request uri {regex {regex name | class class_name} | length gt bytes}**—Matches text found in the HTTP request message URI against the specified regular expression or regular expression class, or messages where the request URI is greater than the specified length.

- **match [not] response body {active-x | java-applet | regex {regex name | class class_name}}**—Matches text found in the HTTP response message body against the specified regular expression or regular expression class, or comments out Java applet and Active X object tags in order to filter them.

- **match [not] response body length gt bytes**—Matches HTTP response messages where the body is greater than the specified length.

- **match [not] response header {field | regex regex_name} regex {regex name | class class_name}**—Matches the content of a field in the HTTP response message header against the specified regular expression or regular expression class. You can specify the field name explicitly or match the field name to a regular expression. Field names are: 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.

- **match [not] response header {field | regex regex_name} {length gt bytes | count gt number}**—Matches the length of the specified fields in the HTTP response message header, or the overall number of fields (count) in the header. You can specify the field name explicitly or match the field name to a regular expression or regular expression class. Field names are listed in the previous bullet.

- **match [not] response header {length gt bytes | count gt number | non-ascii}**—Matches the overall length of the HTTP response message header, or the overall number of fields (count) in the header, or headers that have non-ASCII characters.

- **match [not] response status-line regex {regex name | class class_name}**—Matches text found in the HTTP response message status line against the specified regular expression or regular expression class.

d) Enter **exit** to leave class map configuration mode.

**Step 2**  
Create an HTTP inspection policy map: **policy-map type inspect http policy_map_name**

Where the **policy_map_name** is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 3**  
(Optional) Add a description to the policy map: **description string**

**Step 4**  
To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created an HTTP class map, specify it by entering the following command: **class class_map_name**
• Specify traffic directly in the policy map using one of the `match` commands described for HTTP class maps. If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

• `drop-connection [log]`—Drop the packet and close the connection.
• `reset [log]`—Drop the packet, close the connection, and send a TCP reset to the server or client.
• `log`—Send a system log message. You can use this option alone or with one of the other actions.

You can specify multiple `class` or `match` commands in the policy map. For information about the order of `class` and `match` commands, see How Multiple Traffic Classes are Handled, on page 308.

**Step 5**
To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option:

• `body-match-maximum number`—Sets the maximum number of characters in the body of an HTTP message that should be searched in a body match. The default is 200 bytes. A large number will have a significant impact on performance.

• `protocol-violation action {drop-connection [log] | reset [log] | log}`—Checks for HTTP protocol violations. You must also choose the action to take for violations (drop connection, reset, or log) and whether to enable or disable logging.

• `spoof-server string`—Substitutes a string for the server header field. WebVPN streams are not subject to the spoof-server command.

**Example**
The following example shows how to define an HTTP inspection policy map that will allow and log any HTTP connection that attempts to access “www\.
xyz.com/.*\.asp” or “www\.
xyz[0-9][0-9]\.com” with methods "GET" or "PUT." All other URL/Method combinations will be silently allowed.

```
hostname(config)# regex url1 "www\.xyz.com/.*\.asp"
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"
hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
```

---

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10

345
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 ASA in an ACL. 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.

However, ICMP traffic directed to an ASA interface is never inspected, even if you enable ICMP inspection. Thus, a ping (echo request) to an interface can fail under specific circumstances, such as when the echo request comes from a source that the ASA can reach through a backup default route.

For information on enabling ICMP inspection, see Configure Application Layer Protocol Inspection, on page 315.

ICMP Error Inspection

When ICMP Error inspection is enabled, the ASA creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The ASA overwrites the packet with the translated IP addresses.

When disabled, the ASA 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 ASA 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 ASA. When the ASA does not translate the intermediate hops, all the intermediate hops appear with the mapped destination IP address.

For information on enabling ICMP Error inspection, see Configure Application Layer Protocol Inspection, on page 315.
ILS Inspection

The Internet Locator Service (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. You cannot use PAT with ILS inspection because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, consider using NAT to allow internal peers to communicate locally while registered to external LDAP servers. If you do not need to use NAT, we recommend that you turn off the inspection engine to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the ASA border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Note

Because ILS traffic (H225 call signaling) 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 TCP timeout command. In ASDM, this is on the Configuration > Firewall > Advanced > Global Timeouts pane.

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.

For information on enabling ILS inspection, see Configure Application Layer Protocol Inspection, on page 315.

Instant Messaging Inspection

The Instant Messaging (IM) inspect engine lets you control the network usage of IM and stop leakage of confidential data, propagation of worms, and other threats to the corporate network.

IM inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. However, the default inspect class does include the default IM ports, so you can simply edit the default global inspection policy to add IM inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

If you decide to implement IM inspection, you can also configure an IM inspection policy map to specify actions when a message violates a parameter. The following procedure explains IM inspection policy maps.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.
Procedure

Step 1
(Optional) Create an IM inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the match not command. For example, if the match not command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a) Create the class map: class-map type inspect im [match-all | match-any] class_map_name
   Where the class_map_name is the name of the class map. The match-all keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one match statement. The CLI enters class-map configuration mode, where you can enter one or more match commands.

b) (Optional) Add a description to the class map: description string
   Where string is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following match commands. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

   • match [not] protocol {im-yahoo | im-msn}—Matches a specific IM protocol, either Yahoo or MSN.
   • match [not] service {chat | file-transfer | webcam | voice-chat | conference | games}—Matches the specific IM service.
   • match [not] login-name regex {regex_name | class class_name}—Matches the source client login name of the IM message against the specified regular expression or regular expression class.
   • match [not] peer-login-name regex {regex_name | class class_name}—Matches the destination peer login name of the IM message against the specified regular expression or regular expression class.
   • match [not] ip-address ip_address mask}—Matches the source IP address and mask of the IM message.
   • match [not] peer-ip-address ip_address mask}—Matches the destination IP address and mask of the IM message.
   • match [not] version regex {regex_name | class class_name}—Matches the version of the IM message against the specified regular expression or regular expression class.
   • match [not] filename regex {regex_name | class class_name}—Matches the filename of the IM message against the specified regular expression or regular expression class. This match is not supported for the MSN IM protocol.
d) Enter \texttt{exit} to leave class map configuration mode.

\textbf{Step 2}  
Create an IM inspection policy map: \texttt{policy-map type inspect im policy\_map\_name}

Where the \texttt{policy\_map\_name} is the name of the policy map. The CLI enters policy-map configuration mode.

\textbf{Step 3}  
(Optional) Add a description to the policy map: \texttt{description string}

\textbf{Step 4}  
To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created an IM class map, specify it by entering the following command: \texttt{class class\_map\_name}
- Specify traffic directly in the policy map using one of the \texttt{match} commands described for IM class maps. If you use a \texttt{match not} command, then any traffic that does not match the criterion in the \texttt{match not} command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering the following command:

- \texttt{drop-connection [log]}——Drop the packet and close the connection.
- \texttt{reset [log]}——Drop the packet, close the connection, and send a TCP reset to the server or client.
- \texttt{log}——Send a system log message. You can use this option alone or with one of the other actions.

You can specify multiple \texttt{class} or \texttt{match} commands in the policy map. For information about the order of \texttt{class} and \texttt{match} commands, see \textit{How Multiple Traffic Classes are Handled, on page 308.}

\textbf{Example}

The following example shows how to define an IM inspection policy map.

\verbatiminput{example.txt}

\textbf{CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10}
hostname(config-cmap)# match version regex yahoo_version_regex
hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all

What to do next
You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

IP Options Inspection
You can configure IP Options inspection to control which IP packets are allowed based on the contents of the IP Options field in the packet header. You can drop packets that have unwanted options, clear the options (and allow the packet), or allow the packet without change.

IP options provide control functions that are required in some situations but unnecessary for most common communications. In particular, IP options include provisions for time stamps, security, and special routing. Use of IP Options is optional, and the field can contain zero, one, or more options.

For a list of IP options, with references to the relevant RFCs, see the IANA page, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml.

IP options inspection is enabled by default, but for RSVP traffic only. You need to configure it only if you want to allow additional options than the default map allows, or if you want to apply it to other types of traffic by using a non-default inspection traffic class map.

Note
IP options inspection does not work on fragmented packets. For example, options are not cleared from fragments.

The following sections describe IP Options inspection.

Defaults for IP Options Inspection
IP Options inspection is enabled by default for RSVP traffic only, using the _default_ip_options_map inspection policy map.

• The Router Alert option is allowed.

This option notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols that
Service Policies and Application Inspection

Configure an IP Options Inspection Policy Map

If you want to perform non-default IP options inspection, create an IP options inspection policy map to specify how you want to handle each option type.

Procedure

Step 1 Create an IP options inspection policy map: `policy-map type inspect ip-options policy_map_name`
Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2 (Optional) Add a description to the policy map: `description string`

Step 3 Enter parameters configuration mode:

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

Step 4 Identify the options you want to allow.

You can inspect the following options. In all cases, the `allow` action allows packets that contain the option without modification; the `clear` action allows the packets but removes the option from the header.

Use the `no` form of the command to remove the option from the map. Any packet that contains an option that you do not include in the map is dropped, even if the packet contains otherwise allowed or cleared options.

For a list of IP options, with references to the relevant RFCs, see the IANA page, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml.

- **default action** `{allow | clear}`—Sets the default action for any option not explicitly included in the map. If you do not set a default action of allow or clear, packets that contain non-allowed options are dropped.
- **basic-security action** `{allow | clear}`—Allows or clears the Security (SEC) option.
- **commercial-security action** `{allow | clear}`—Allows or clears the Commercial Security (CIPSO) option.
- **eool action** `{allow | clear}`—Allows or clears the End of Options List option.
IPsec Pass Through Inspection

IPsec Pass Through inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. However, the default inspect class does include the default IPsec ports, so you can simply edit the default global inspection policy to add IPsec inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

The following sections describe the IPsec Pass Through inspection engine.

IPsec Pass Through Inspection Overview

Internet Protocol Security (IPsec) is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (for example, computer users or servers), between a pair of security gateways (such as routers or firewalls), or between a security gateway and a host.

IPsec Pass Through application inspection provides convenient traversal of ESP (IP protocol 50) and AH (IP protocol 51) traffic associated with an IKE UDP port 500 connection. It avoids lengthy ACL configuration to permit ESP and AH traffic and also provides security using timeout and max connections.

Configure a policy map for IPsec Pass Through to specify the restrictions for ESP or AH traffic. You can set the per client max connections and the idle timeout.
NAT and non-NAT traffic is permitted. However, PAT is not supported.

**Configure an IPsec Pass Through Inspection Policy Map**

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 ACL.

The configuration includes a default map, `_default_ipsec_passthru_map`, that sets no maximum limit on ESP connections per client, and sets the ESP idle timeout at 10 minutes. You need to configure an inspection policy map only if you want different values, or if you want to set AH values.

**Procedure**

**Step 1**
Create an IPsec Pass Through inspection policy map: `policy-map type inspect ipsec-pass-thru policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2**
(Optional) Add a description to the policy map: `description string`

**Step 3**
To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option:

- **esp per-client-max number timeout time**—Allows ESP tunnels and sets the maximum connections allowed per client and the idle timeout (in hh:mm:ss format). To allow an unlimited number of connections, specify 0 for the number.

- **ah per-client-max number timeout time**—Allows AH tunnels. The parameters have the same meaning as for the `esp` command.

**Example**

The following example shows how to use ACLs to identify IKE traffic, define an IPsec Pass Thru parameter map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
```
IPv6 Inspection

IPv6 inspection lets you selectively log or drop IPv6 traffic based on the extension header. In addition, IPv6 inspection can check conformance to RFC 2460 for type and order of extension headers in IPv6 packets. IPv6 inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add IPv6 inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

Defaults for IPv6 Inspection

If you enable IPv6 inspection and do not specify an inspection policy map, then the default IPv6 inspection policy map is used, and the following actions are taken:

- Allows only known IPv6 extension headers. Non-conforming packets are dropped and logged.
- Enforces the order of IPv6 extension headers as defined in the RFC 2460 specification. Non-conforming packets are dropped and logged.
- Drops any packet with a routing type header.

Following is the policy map configuration:

```
policy-map type inspect ipv6 _default_ipv6_map
description Default IPV6 policy-map
parameters
  verify-header type
  verify-header order
match header routing-type range 0 255
  drop log
```

Configure an IPv6 Inspection Policy Map

To identify extension headers to drop or log, or to disable packet verification, create an IPv6 inspection policy map to be used by the service policy.

**Procedure**

**Step 1**
Create an IPv6 inspection policy map: `policy-map type inspect ipv6 policy_map_name`
Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2**
(Optional) Add a description to the policy map: `description string`

**Step 3**
(Optional) Drop or log traffic based on the headers in IPv6 messages.

a) Identify the traffic based on the IPv6 header: `match header type`
Where `type` is one of the following:
Configure an IPv6 Inspection Policy Map

1. Configure the inspection engine.
   a) Enter parameters configuration mode.

   ```
   hostname(config-pmap)# parameters
   hostname(config-pmap-p)#
   ```

   b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:

   - **verify-header type**—Allows only known IPv6 extension headers.
   - **verify-header order**—Enforces the order of IPv6 extension headers as defined in RFC 2460.

2. Configure parameters that affect the inspection engine.
   a) Enter parameters configuration mode.

   ```
   hostname(config-pmap)# parameters
   hostname(config-pmap-p)#
   ```

   b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:

   - **verify-header type**—Allows only known IPv6 extension headers.
   - **verify-header order**—Enforces the order of IPv6 extension headers as defined in RFC 2460.

3. Specify the action to perform on matching packets. You can drop the packet and optionally log it, or just log it. If you do not enter an action, the packet is logged.

   - **drop [log]**—Drop all packets that match.
   - **log**—Send a system log message. You can use this option alone or with one of the other actions.

4. Repeat the process until you identify all headers that you want to drop or log.

Example

The following example creates an inspection policy map that will drop and log all IPv6 packets with the hop-by-hop, destination-option, routing-address, and routing type 0 headers. It also enforces header order and type.

```bash
policy-map type inspect ipv6 ipv6-pm
parameters
  verify-header type
  verify-header order
match header hop-by-hop
  drop log
match header destination-option
```
NetBIOS Inspection

NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service (NBNS) packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.

NetBIOS inspection is enabled by default. You can optionally create a policy map to drop or log NetBIOS protocol violations. The following procedure explains how to configure a NetBIOS inspection policy map.

Procedure

**Step 1**
Create a NetBIOS inspection policy map: `policy-map type inspect netbios policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2**
(Optional) Add a description to the policy map: `description string`

**Step 3**
Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

**Step 4**
Specify the action to take for NETBIOS protocol violations: `protocol-violation action {drop [log] | log}`

Where the `drop` action drops the packet. The `log` action sends a system log message when this policy map matches traffic.

**Example**

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log
```
hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# no inspect netbios
hostname(config-pmap-c)# inspect netbios netbios_map

What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

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 carry 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.

Specifically, the ASA 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 dynamically 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).

For information on enabling PPTP inspection, see Configure Application Layer Protocol Inspection, on page 315.

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.

For information on enabling RSH inspection, see Configure Application Layer Protocol Inspection, on page 315.

SMTP and Extended SMTP Inspection

ESMTP inspection detects attacks, including spam, phising, malformed message attacks, and buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforces the sanity of the ESMTP messages as well as block senders/receivers, and block mail relay.

ESMTP inspection is enabled by default. You need to configure it only if you want different processing than that provided by the default inspection map.
The following sections describe the ESMTP inspection engine.

SMTP and ESMTP Inspection Overview

Extended SMTP (ESMTP) application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the ASA and by adding monitoring capabilities. ESMTP is an enhancement to the SMTP protocol and is similar in most respects to SMTP.

ESMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. ESMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands. Supported commands are the following:
  - Extended SMTP—AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS, and VRFY.
  - SMTP (RFC 821)—DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

ESMTP 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 or unsupported commands, the inspection engine changes all the characters in the packet to X, which are rejected by the internal server. This results in a message such as “500 Command unknown: ‘XXXX’. ” Incomplete commands are discarded
  Unsupported ESMTP commands are ATRN, ONEX, VERB, CHUNKING, and private extensions.
- TCP stream editing.
- Command pipelining.

With ESMTP 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; they must be terminated with carriage return and line feed; and you must wait for a response before issuing the next reply.

Defaults for ESMTP Inspection

ESMTP inspection is enabled by default, using the _default_esmtp_map inspection policy map.
• The server banner is masked. The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “0” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

• Encrypted connections are allowed but not inspected.

• Special characters in sender and receiver address are not noticed, no action is taken.

• Connections with command line length greater than 512 are dropped and logged.

• Connections with more than 100 recipients are dropped and logged.

• Messages with body length greater than 998 bytes are logged.

• Connections with header line length greater than 998 are dropped and logged.

• Messages with MIME filenames greater than 255 characters are dropped and logged.

• EHLO reply parameters matching “others” are masked.

Following is the policy map configuration:

```
policy-map type inspect esmtp _default_esmtp_map
description Default ESMTP policy-map
parameters
  mask-banner
  no mail-relay
  no special-character
  allow-tls
match cmd line length gt 512
drop-connection log
match cmd RCPT count gt 100
drop-connection log
match body line length gt 998
log
match header line length gt 998
drop-connection log
match sender-address length gt 320
drop-connection log
match MIME filename length gt 255
drop-connection log
match ehlo-reply-parameter others
mask
```

### Configure an ESMTP Inspection Policy Map

To specify actions when a message violates a parameter, create an ESMTP inspection policy map. You can then apply the inspection policy map when you enable ESMTP inspection.

#### Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.
Procedure

Step 1  Create an ESMTP inspection policy map: `policy-map type inspect esmtp policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2  (Optional) Add a description to the policy map: `description string`

Step 3  To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following `match` commands. If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

  - `match [not] body {length | line length} gt bytes`—Matches messages where the length or length of a line in an ESMTP body message is greater than the specified number of bytes.
  - `match [not] cmd verb verb1 [verb2...]`—Matches the command verb in the message. You can specify one or more of the following commands: auth, data, ehlo, etrn, helo, help, mail, noop, quit, rcpt, rset, saml, soml, vrfy.
  - `match [not] cmd line length gt bytes`—Matches messages where the length of a line in the command verb is greater than the specified number of bytes.
  - `match [not] cmd rcpt count gt count`—Matches messages where the number of recipients is greater than the specified count.
  - `match [not] ehlo-reply-parameter parameter [parameter2...]`—Matches ESMTP EHLO reply parameters. You can specify one or more of the following parameters: 8bitmime, auth, binaryname, checkpoint, dsn, etrn, others, pipelining, size, vrfy.
  - `match [not] header {length | line length} gt bytes`—Matches messages where the length or length of a line in an ESMTP header is greater than the specified number of bytes.
  - `match [not] header to-fields count gt count`—Matches messages where the number of To fields in the header is greater than the specified number.
  - `match [not] invalid-recipients count gt number`—Matches messages where the number of invalid recipients is greater than the specified count.
  - `match [not] mime filetype regex {regex_name | class class_name}`—Matches the MIME or media file type against the specified regular expression or regular expression class.
  - `match [not] mime filename length gt bytes`—Matches messages where a file name is longer than the specified number of bytes.
  - `match [not] mime encoding type [type2...]`—Matches the MIME encoding type. You can specify one or more of the following types: 7bit, 8bit, base64, binary, others, quoted-printable.
  - `match [not] sender-address regex {regex_name | class class_name}`—Matches the sender email address against the specified regular expression or regular expression class.
  - `match [not] sender-address length gt bytes`—Matches messages where the sender address is greater than the specified number of bytes.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

  - `drop-connection [log]`—Drop the packet and close the connection.
Service Policies and Application Inspection

Configure an ESMTP Inspection Policy Map

- **mask [log]**—Mask out the matching portion of the packet. This action is available for `ehlo-reply-parameter` and `cmd verb` only.
- **reset [log]**—Drop the packet, close the connection, and send a TCP reset to the server or client.
- **log**—Send a system log message. You can use this option alone or with one of the other actions.
- **rate-limit message_rate**—Limit the rate of messages in packets per second. This option is available with `cmd verb` only, where you can use it as the only action, or you can use it in conjunction with the `mask` action.

You can specify multiple **match** commands in the policy map. For information about the order of **match** commands, see How Multiple Traffic Classes are Handled, on page 308.

**Step 4**

To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option:

- **mail-relay domain-name action {drop-connection [log] [log]}**—Identifies a domain name for mail relay. You can either drop the connection and optionally log it, or log it.
- **mask-banner**—_masks the banner from the ESMTP server.
- **special-character action {drop-connection [log] [log]}**—Identifies the action to take for messages that include the special characters pipe (|), back quote, and NUL in the sender or receiver email addresses. You can either drop the connection and optionally log it, or log it.
- **allow-tls [action log]**—Whether to allow ESMTP over TLS (encrypted connections) without inspection. You can optionally log encrypted connections. The default is to allow TLS sessions without inspection. If you specify **no allow-tls**, the system strips the STARTTLS indication from the session connection and forces a plain-text connection.

**Example**

The following example shows how to define an ESMTP inspection policy map.

```
hostname(config)# regex user1 “user1@cisco.com”
hostname(config)# regex user2 “user2@cisco.com”
hostname(config)# regex user3 “user3@cisco.com”
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description “Regular expressions to filter out undesired senders”
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class Senders_black_list
```
hostname(config-pmap-c)# drop-connection log
hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map
hostname(config)# service-policy outside_policy interface outside

What to do next
You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

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 ASA can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map.

SNMP inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add SNMP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

Procedure

Create an SNMP map.

Use the `snmp-map map_name` command to create the map and enter SNMP map configuration mode, then the `deny version version` command to identify the versions to disallow. The version can be 1, 2, 2c, or 3.

Example:
The following example denies SNMP Versions 1 and 2:

hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2

What to do next
You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.
SQL*Net Inspection

SQL*Net inspection is enabled by default. The inspection engine supports SQL*Net versions 1 and 2, but only the Transparent Network Substrate (TNS) format. Inspection does not support the Tabular Data Stream (TDS) format. SQL*Net messages are scanned for embedded addresses and ports, and NAT rewrite is applied when necessary.

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). If your application uses a different port, apply the SQL*Net inspection to a traffic class that includes that port.

---

**Note**

Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

For information on enabling SQL*Net inspection, see Configure Application Layer Protocol Inspection, on page 315.

Sun RPC Inspection

This section describes Sun RPC application inspection.

Sun RPC Inspection Overview

Sun RPC protocol inspection is enabled by default. You simply need to manage the Sun RPC server table to identify which services are allowed to traverse the firewall. However, pinholing for NFS is done for any server even without the server table configuration.

Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access a 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 ASA intercepts this packet and opens both embryonic TCP and UDP connections on that port.

NAT or PAT of Sun RPC payload information is not supported.

Manage Sun RPC Services

Use the Sun RPC services table to control Sun RPC traffic based on established Sun RPC sessions.

**Procedure**

**Step 1** Configure the Sun RPC service properties.
sunrpc-server interface_name ip_address mask service service_type protocol {tcp | udp} port[-port] timeout hh:mm:ss

Where:

- **interface_name**—The interface through which traffic to the server flows.
- **ip_address mask**—The address of the Sun RPC server.
- **service service_type**—The service type on the server, which is the mapping between a specific service type and the port number used for the service. To determine the service type (for example, 100003), use the `sunrpcinfo` command at the UNIX or Linux command line on the Sun RPC server machine.
- **protocol {tcp | udp}**—Whether the service uses TCP or UDP.
- **port[-port]**—The port or range of ports used by the service. To specify a range of ports, separate the starting and ending port numbers in the range with a hyphen (for example, 111-113).
- **timeout hh:mm:ss**—The idle timeout for the pinhole opened for the connection by Sun RPC inspection.

**Example:**

For example, to create a timeout of 30 minutes to the Sun RPC server with the IP address 192.168.100.2, enter the following command. In this example, the Sun RPC server is on the inside interface using TCP port 111.

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol tcp 111 timeout 00:30:00
```

**Step 2** *(Optional.)* Monitor the pinholes created for these services.

To display the pinholes open for Sun RPC services, enter the `show sunrpc-server active` command. For example:

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

If necessary, you can clear these services using the `clear sunrpc-server active` command.

---

**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 inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR), and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server.

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.

For information on enabling TFTP inspection, see Configure Application Layer Protocol Inspection, on page 315.

**XDMCP Inspection**

XDMCP inspection is enabled by default. 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 ASA must allow the TCP back connection from the Xhosted computer. To permit the back connection, you can use access rules to allow the TCP ports. Alternatively, you can use the `established` command on the ASA. 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 ASA can NAT if needed. XDCMP inspection does not support PAT.

For information on enabling XDMCP inspection, see Configure Application Layer Protocol Inspection, on page 315.

**VXLAN Inspection**

Virtual Extensible Local Area Network (VXLAN) inspection works on VXLAN encapsulated traffic that passes through the ASA. It ensures that the VXLAN header format conforms to standards, dropping any malformed packets. VXLAN inspection is not done on traffic for which the ASA acts as a VXLAN Tunnel End Point (VTEP) or a VXLAN gateway, as those checks are done as a normal part of decapsulating VXLAN packets.

VXLAN packets are UDP, normally on port 4789. This port is part of the default-inspection-traffic class, so you can simply add VXLAN inspection to the inspection_default service policy rule. Alternatively, you can create a class for it using port or ACL matching.
## History for Basic Internet Protocol Inspection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.</td>
<td>9.4(1)</td>
<td>The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any commands.</td>
</tr>
<tr>
<td>VXLAN packet inspection</td>
<td>9.4(1)</td>
<td>The ASA can inspect the VXLAN header to enforce compliance with the standard format. We introduced the following command: inspect vxlan.</td>
</tr>
<tr>
<td>ESMTP inspection change in default behavior for TLS sessions.</td>
<td>9.4(1)</td>
<td>The default for ESMTP inspection was changed to allow TLS sessions, which are not inspected. However, this default applies to new or reimaged systems. If you upgrade a system that includes no allow-tls, the command is not changed. The change in default behavior was also made in these older versions: 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).</td>
</tr>
<tr>
<td>IP Options inspection improvements.</td>
<td>9.5(1)</td>
<td>IP Options inspection now supports all possible IP options. You can tune the inspection to allow, clear, or drop any standard or experimental options, including those not yet defined. You can also set a default behavior for options not explicitly defined in an IP options inspection map. We added the following commands: basic-security, commercial-security, default, exp-flow-control, exp-measure, extended-security, imi-traffic-description, quick-start, record-route, timestamp, and {0-255} (which indicates an IP option type number).</td>
</tr>
<tr>
<td>DCERPC inspection improvements and UUID filtering</td>
<td>9.5(2)</td>
<td>DCERPC inspection now supports NAT for OXidResolver ServerAlive2 opnum5 messages. You can also now filter on DCERPC message universally unique identifiers (UUIDs) to reset or log particular message types. There is a new DCERPC inspection class map for UUID filtering. We introduced the following command: match [not] uuid. We modified the following command: class-map type inspect.</td>
</tr>
<tr>
<td>DNS over TCP inspection.</td>
<td>9.6(2)</td>
<td>You can now inspect DNS over TCP traffic (TCP/53). We added the following command: tcp-inspection.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco Umbrella support.</td>
<td>9.10(1)</td>
<td>You can configure the device to redirect DNS requests to Cisco Umbrella, so that your Enterprise Security policy defined in Cisco Umbrella can be applied to user connections. You can allow or block connections based on FQDN, or for suspicious FQDNs, you can redirect the user to the Cisco Umbrella intelligent proxy, which can perform URL filtering. The Umbrella configuration is part of the DNS inspection policy. We added or modified the following commands: <code>umbrella</code> (global and policy-map parameters configuration modes), <code>token</code>, <code>public-key</code>, <code>timeout edns</code>, <code>dnscrypt</code>, <code>show service-policy inspect dns detail</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 16

Inspection for Voice and Video Protocols

The following topics explain application inspection for voice and video protocols. For basic information on why you need to use inspection for certain protocols, and the overall methods for applying inspection, see Getting Started with Application Layer Protocol Inspection, on page 307.

- CTIQBE Inspection, on page 369
- H.323 Inspection, on page 370
- MGCP Inspection, on page 375
- RTSP Inspection, on page 378
- SIP Inspection, on page 381
- Skinny (SCCP) Inspection, on page 386
- STUN Inspection, on page 389
- History for Voice and Video Protocol Inspection, on page 390

CTIQBE Inspection

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 ASA.

TAPI and JTAPI are used by many Cisco VoIP applications. CTIQBE is used by Cisco TSP to communicate with Cisco CallManager.

For information on enabling CTIQBE inspection, see Configure Application Layer Protocol Inspection, on page 315.

Limitations for CTIQBE Inspection

Stateful failover of CTIQBE calls is not supported.

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 ASA, calls between these two phones fail.

- 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.

## H.323 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.

H.323 inspection is enabled by default. You need to configure it only if you want non-default processing. The following sections describe the H.323 application inspection.

### H.323 Inspection Overview

H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The ASA supports H.323 through Version 6, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the ASA 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 ASA.

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 ASA uses an ASN.1 decoder to decode the H.323 messages.
- Dynamically allocate the negotiated H.245 and RTP/RTCP connections. The H.225 connection can also be dynamically allocated when using RAS.

### How H.323 Works

The H.323 collection of protocols collectively may use up to two TCP connection and four to eight UDP connections. FastConnect uses only one TCP connection, and RAS uses a single UDP connection for registration, admissions, and status.

An H.323 client can 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 ASA dynamically allocates the H.245 connection based on the inspection of the H.225 messages. The H.225 connection can also be dynamically allocated when using RAS.
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 1719 for RAS signaling. Additionally, 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 ASA opens an H.225 connection based on inspection of the ACF and RCF messages.

After inspecting the H.225 messages, the ASA opens the H.245 channel and then inspects traffic sent over the H.245 channel as well. All H.245 messages passing through the ASA undergo H.245 application inspection, which translates embedded IP addresses and opens the media channels negotiated in H.245 messages.

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 with the `timeout` command.

---

**Note**

You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The ASA includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the ASA opens a pinhole through source IP address/port 0/0. By default, this option is disabled. To enable call setup between H.323 endpoint, enter the `ras-rcf-pinholes enable` command during parameter configuration mode while creating an H.323 Inspection policy map.

---

**H.239 Support in H.245 Messages**

The ASA sits between two H.323 endpoints. When the two H.323 endpoints set up a telepresentation session so that the endpoints can send and receive a data presentation, such as spreadsheet data, the ASA ensure successful H.239 negotiation between the endpoints.

H.239 is a standard that provides the ability for H.300 series endpoints to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel.

The ASA opens pinholes for the additional media channel and the media control channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13.

The decoding and encoding of the telepresentation session is enabled by default. H.239 encoding and decoding is performed by ASN.1 coder.
Limitations for H.323 Inspection

H.323 inspection is tested and supported for Cisco Unified Communications Manager (CUCM) 7.0. It is not supported for CUCM 8.0 and higher. H.323 inspection might work with other releases and products.

The following are some of the known issues and limitations when using H.323 application inspection:

- PAT is supported except for extended PAT or per-session PAT.
- 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.
- Not supported with NAT between same-security-level interfaces.
- Not supported with NAT64.
- NAT with H.323 inspection is not compatible with NAT when done directly on the endpoints. If you perform NAT on the endpoints, disable H.323 inspection.

Configure H.323 Inspection Policy Map

You can create an H.323 inspection policy map to customize H.323 inspection actions if the default inspection behavior is not sufficient for your network.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

Procedure

Step 1

(Optional) Create an H.323 inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the match not command. For example, if the match not command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a) Create the class map: class-map type inspect h323 [match-all | match-any] class_map_name

   Where class_map_name is the name of the class map. The match-all keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one of the criteria. The CLI enters class-map configuration mode, where you can enter one or more match commands.

b) (Optional) Add a description to the class map: description string
Service Policies and Application Inspection

Where string is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following match commands. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

- **match [not] called-party regex {regex_name | class class_name}**—Matches the called party against the specified regular expression or regular expression class.

- **match [not] calling-party regex {regex_name | class class_name}**—Matches the calling party against the specified regular expression or regular expression class.

- **match [not] media-type {audio | data | video}**—Matches the media type.

**Step 2**
Create an H.323 inspection policy map: `policy-map type inspect h323 policy_map_name`

Where the **policy_map_name** is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 3**
(Optional) Add a description to the policy map: `description string`

**Step 4**
To apply actions to matching traffic, perform the following steps.

You can specify multiple class or match commands in the policy map. For information about the order of class and match commands, see How Multiple Traffic Classes are Handled, on page 308.

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created an H.323 class map, specify it by entering the following command: `class class_map_name`

- Specify traffic directly in the policy map using one of the match commands described for H.323 class maps. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

- **drop [log]**—Drop the packet. For media type matches, you can include the log keyword to send a system log message.

- **drop-connection**—Drop the packet and close the connection. This option is available for called or calling party matching.

- **reset**—Drop the packet, close the connection, and send a TCP reset to the server and/or client. This option is available for called or calling party matching.

**Step 5**
To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:

- **ras-rcf-pinholes enable**—Enables call setup between H.323 endpoints. You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. Use this option to open pinholes
for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the ASA opens a pinhole through source IP address/port 0/0. By default, this option is disabled.

- **timeout users time**—Sets the H.323 call duration limit (in hh:mm:ss format). To have no timeout, specify 00:00:00. Range is from 0:0:0 to 1193:0:0.

- **call-party-number**—Enforces sending call party number during call setup.

- **h245-tunnel-block action {drop-connection | log}**—Enforces H.245 tunnel blocking. Specify whether you want to drop the connection or simply log it.

- **rtp-conformance [enforce-payloaddtype]**—Checks RTP packets flowing on the pinholes for protocol conformance. The optional enforce-payloaddtype keyword enforces the payload type to be audio or video based on the signaling exchange.

- **state-checking {h225 | ras}**—Enables state checking validation. You can enter the command separately to enable state checking for H.225 and RAS.

- **early-message message_type**—Whether to allow the specified type of H.225 messages before the H.225 SETUP message. You can allow the facility message to arrive early, in compliance with H.460.18.

If you encounter call setup issues, where connections are being closed before being completed when using H.323/H.225, use this command to allow early messages. Also, ensure that you enable inspection for both H.323 RAS and H.225 (they are both enabled by default).

### Step 6

While still in parameter configuration mode, you can configure HSI groups.

a) Define an HSI group and enter HSI group configuration mode: `hsi-group id`

   Where *id* is the HSI group ID. Range is from 0 to 2147483647.

b) Add an HSI to the HSI group using the IP address: `hsi ip_address`

   You can add a maximum of five hosts per HSI group.

c) Add an endpoint to the HSI group: `endpoint ip_address if_name`

   Where *ip_address* is the endpoint to add and *if_name* is the interface through which the endpoint is connected to the ASA. You can add a maximum of ten endpoints per HSI group.

### Example

The following example shows how to configure phone number filtering:

```bash
hostname(config)# regex caller 1 "5551234567"
hosname(config)# regex caller 2 "5552345678"
hosname(config)# regex caller 3 "5553456789"
hosname(config)# class-map type inspect h323 match-all h323_traffic
hosname(config-pmap-c)# match called-party regex caller1
hosname(config-pmap-c)# match calling-party regex caller2
```
What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

MGCP Inspection

MGCP inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. However, the default inspect class does include the default MGCP ports, so you can simply edit the default global inspection policy to add MGCP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

The following sections describe MGCP application inspection.

MGCP Inspection Overview

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. The following figure illustrates how you can use 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.

- Gateways usually listen to UDP port 2427 to receive commands from the call agent.
- The port on which the call agent receives commands from the gateway. Call agents usually listen to UDP port 2727 to receive commands from the gateway.

**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 ASA requires the RTP data to come from the same address as MGCP signaling.

### Configure an MGCP Inspection Policy Map

If the network has multiple call agents and gateways for which the ASA has to open pinholes, create an MGCP map. You can then apply the MGCP map when you enable MGCP inspection.

#### Procedure

**Step 1**

To create an MGCP inspection policy map: `policy-map type inspect mgcp policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.
Step 2  (Optional) Add a description to the policy map: `description string`

Step 3  Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

Step 4  Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option.

- **call-agent ip_address group_id**—Configures the call agent groups that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. Call agents with the same group_id belong to the same group. A call agent may belong to more than one group. The group_id option is a number from 0 to 4294967295. The ip_address option specifies the IP address of the call agent.

  **Note**  MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the ASA and allows MGCP end points to register with the call agent.

- **gateway ip_address group_id**—Identifies which group of call agents is managing a particular gateway. The IP address of the gateway is specified with the ip_address option. The group_id option is a number from 0 to 4294967295 that must correspond with the group_id of the call agents that are managing the gateway. A gateway may only belong to one group.

- **command-queue command_limit**—Sets the maximum number of commands allowed in the MGCP command queue, from 1 to 2147483647. The default is 200.

---

**Example**

The following example shows how to define an MGCP map:

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

**What to do next**

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.
RTSP Inspection

RTSP inspection is enabled by default. You need to configure it only if you want non-default processing. The following sections describe RTSP application inspection.

RTSP Inspection Overview

The RTSP inspection engine lets the ASA 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 ports 554 and 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The ASA only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that are 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 ASA parses Setup response messages with a status code of 200. If the response message is traveling inbound, the server is outside relative to the ASA and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the ASA does not need to open dynamic channels.

RTSP inspection does not support PAT or dual-NAT. Also, the ASA cannot recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.

RealPlayer Configuration Requirements

When using RealPlayer, it is important to properly configure transport mode. For the ASA, add an access-list command 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 ASA, 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 ASA, add an inspect rtsp command.

Limitations for RSTP Inspection

The following restrictions apply to the RSTP inspection.

- The ASA does not support multicast RTSP or RTSP messages over UDP.
- The ASA does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The ASA 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 the ASA cannot perform NAT on fragmented packets.

- With Cisco IP/TV, the number of translates the ASA 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.

## Configure RTSP Inspection Policy Map

You can create an RTSP inspection policy map to customize RTSP inspection actions if the default inspection behavior is not sufficient for your network.

### Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

### Procedure

**Step 1**

(Optional) Create an RTSP inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the match not command. For example, if the match not command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a) Create the class map: `class-map type inspect rtsp [match-all | match-any] class_map_name`

   Where `class_map_name` is the name of the class map. The match-all keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one of the criteria. The CLI enters class-map configuration mode, where you can enter one or more match commands.

b) (Optional) Add a description to the class map: `description string`

   Where `string` is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following match commands. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.
Configure RTSP Inspection Policy Map

- **match [not] request-method **method**—Matches an RTSP request method. The methods are: announce, describe, get-parameter, options, pause, play, record, redirect, setup, set-parameter, teardown.
- **match [not] url-filter regex** \{regex_name | class class_name\}—Matches the URL against the specified regular expression or regular expression class.

**Step 2**
To create an RTSP inspection policy map: policy-map type inspect rtsp policy_map_name
Where the policy_map_name is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 3**
(Optional) Add a description to the policy map: description string

**Step 4**
To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:
   - If you created an RTSP class map, specify it by entering the following command: class class_map_name
   - Specify traffic directly in the policy map using one of the **match** commands described for RTSP class maps. If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:
   - **drop-connection [log]**—Drop the packet, close the connection, and optionally send a system log message. This option is available for URL matching.
   - **log**—Send a system log message.
   - **rate-limit message_rate**—Limit the rate of messages per second. This option is available for request method matching.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see How Multiple Traffic Classes are Handled, on page 308.

**Step 5**
To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:
   - **reserve-port-protect**—Restricts the use of reserve ports during media negotiation.
   - **url-length-limit bytes**—Sets a limit on the URL length allowed in the message, from 0 to 6000 bytes.

---

**Example**
The following example shows a how to define an RTSP inspection policy map.
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global

What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

SIP 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.

SIP inspection is enabled by default. You need to configure it only if you want non-default processing, or if you want to identify a TLS proxy to enable encrypted traffic inspection. The following topics explain SIP inspection in more detail.

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 signaling. SDP specifies the ports for the media stream. Using SIP, the ASA can support any SIP VoIP gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 3261
- SDP: Session Description Protocol, RFC 2327
To support SIP calls through the ASA, 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. Note that the maximum length of the SIP Request URI that the ASA supports is 255.

Instant Messaging (IM) applications also use SIP extensions (defined in RFC 3428) and SIP-specific event notifications (RFC 3265). After users initiate a chat session (registration/subscription), the IM applications use the MESSAGE/INFO methods and 202 Accept responses when users chat with each other. 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**

SIP inspection supports the Chat feature only. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

### Limitations for SIP Inspection

SIP inspection is tested and supported for Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6, and 10.5. It is not supported for CUCM 8.5, or 9.x. SIP inspection might work with other releases and products.

SIP inspection applies NAT for embedded IP addresses. However, if you configure NAT to translate both source and destination addresses, the external address (“from” in the SIP header for the “trying” response message) is not rewritten. Thus, you should use object NAT when working with SIP traffic so that you avoid translating the destination address.

Do not configure NAT or PAT for interfaces with the same, or lower (source) to higher (destination), security levels. This configuration is not supported.

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 ASA, 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. Because PAT needs a port to translate, the translation fails.

- When using PAT, any SIP header field which contains an internal IP address without a port might not be translated and hence the internal IP address will be leaked outside. If you want to avoid this leakage, configure NAT instead of PAT.
Default SIP Inspection

SIP inspection is enabled by default using the default inspection map, which includes the following:

- 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.

Also note that inspection of encrypted traffic is not enabled. You must configure a TLS proxy to inspect encrypted traffic.

Configure SIP Inspection Policy Map

You can create a SIP inspection policy map to customize SIP inspection actions if the default inspection behavior is not sufficient for your network.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

Procedure

Step 1

(Optional) Create a SIP inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify match commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the match not command. For example, if the match not command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each match command, you should identify the traffic directly in the policy map.

a) Create the class map: class-map type inspect sip [match-all | match-any] class_map_name

Where the class_map_name is the name of the class map. The match-all keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one match statement. The CLI enters class-map configuration mode, where you can enter one or more match commands.
b) (Optional) Add a description to the class map: description string

Where string is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following match commands. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

- match [not] called-party regex {regex_name | class class_name}—Matches the called party, as specified in the To header, against the specified regular expression or regular expression class.
- match [not] calling-party regex {regex_name | class class_name}—Matches the calling party, as specified in the From header, against the specified regular expression or regular expression class.
- match [not] content length gt bytes—Matches messages where the content length in the SIP header is greater than the specified number of bytes, from 0 to 65536.
- match [not] content type {sdp | regex {regex_name | class class_name}}—Matches the content type as SDP or against the specified regular expression or regular expression class.
- match [not] im-subscriber regex {regex_name | class class_name}—Matches the SIP IM subscriber against the specified regular expression or regular expression class.
- match [not] message-path regex {regex_name | class class_name}—Matches the SIP via header against the specified regular expression or regular expression class.
- match [not] third-party-registration regex {regex_name | class class_name}—Matches the requester of a third-party registration against the specified regular expression or regular expression class.
- match [not] uri {sip | tel} length gt bytes—Matches a URI in the SIP headers of the selected type (SIP or TEL) that is greater than the length specified, between 0 and 65536 bytes.

d) Enter exit to leave class map configuration mode.

Step 2 Create a SIP inspection policy map: policy-map type inspect sip policy_map_name

Where the policy_map_name is the name of the policy map. The CLI enters policy-map configuration mode.

Step 3 (Optional) Add a description to the policy map: description string

Step 4 To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:

- If you created a SIP class map, specify it by entering the following command: class class_map_name

- Specify traffic directly in the policy map using one of the match commands described for SIP class maps. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

- drop—Drop all packets that match.
- drop-connection—Drop the packet and close the connection.
- reset—Drop the packet, close the connection, and send a TCP reset to the server and/or client.
Step 5  To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option:

- **im**—Enables instant messaging.
- **ip-address-privacy**—Enables IP address privacy, which hides the server and endpoint IP addresses.
- **max-forwards-validation action** {drop | drop-connection | reset | log} [log]
  - Checks the value of the Max-Forwards header, which cannot be zero before reaching the destination. You must also choose the action to take for non-conforming traffic (drop packet, drop connection, reset, or log) and whether to enable or disable logging.
- **rtp-conformance [enforce-payloadtype]**—Checks RTP packets flowing on the pinholes for protocol conformance. The optional enforce-payloadtype keyword enforces the payload type to be audio or video based on the signaling exchange.
- **software-version action** {mask [log] | log}
  - Identifies the software version using the Server and User-Agent (endpoint) header fields. You can mask the software version in the SIP messages and optionally log it, or simply log it.
- **state-checking action** {drop | drop-connection | reset | log} [log]
  - Enables state transition checking. You must also choose the action to take for non-conforming traffic (drop packet, drop connection, reset, or log) and whether to enable or disable logging.
- **strict-header-validation action** {drop | drop-connection | reset | log} [log]
  - Enables strict verification of the header fields in the SIP messages according to RFC 3261. You must also choose the action to take for non-conforming traffic (drop packet, drop connection, reset, or log) and whether to enable or disable logging.
- **traffic-non-sip**—Allows non-SIP traffic on the well-known SIP signaling port.
- **trust-verification-server ip ip_address**—Identifies Trust Verification Services servers, which enable Cisco Unified IP Phones to authenticate application servers during HTTPS establishment. You can enter the command up to four times to identify four servers. SIP inspection opens pinholes to each server for each registered phone, and the phone decides which to use. Configure the Trust Verification Services server on the CUCM server.
- **trust-verification-server port number**—Identifies the Trust Verification Services port. The default port is 2445, so use this command only if the server uses a different port. The allowed port range is 1026 to 32768.
• **uri-non-sip action** `{mask [log] | log}`—Identifies the non-SIP URIs present in the Alert-Info and Call-Info header fields. You can mask the information in the SIP messages and optionally log it, or simply log it.

### Examples

The following example shows how to disable instant messaging over SIP:

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im
```

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap
```

```
hostname(config)# service-policy global_policy global
```

The following example shows how to identify four Trust Verification Services servers.

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

### What to do next

You can now configure an inspection policy to use the map. See **Configure Application Layer Protocol Inspection**, on page 315.

## Skinny (SCCP) Inspection

SCCP (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.

SCCP inspection is enabled by default. You need to configure it only if you want non-default processing, or if you want to identify a TLS proxy to enable encrypted traffic inspection.

The following sections describe SCCP application inspection.

### 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.
The ASA 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 signaling and media packets can traverse the ASA.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The ASA 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.

**Note**
The ASA supports inspection of traffic from Cisco IP Phones running SCCP protocol version 22 and earlier.

### Supporting Cisco IP Phones

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. A 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 ACL 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 ACL or static entry is required to allow the Cisco IP Phones to initiate the connection.

### Limitations for SCCP Inspection

SCCP inspection is tested and supported for Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6, and 10.5. It is not supported for CUCM 8.5, or 9.x. SCCP inspection might work with other releases and products.

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 ASA does not support NAT or PAT for the file content transferred over TFTP. Although the ASA supports NAT of TFTP messages and opens a pinhole for the TFTP file, the ASA 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 ASA supports stateful failover of SCCP calls except for calls that are in the middle of call setup.

### Default SCCP Inspection

SCCP inspection is enabled by default using these defaults:
• 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.

Also note that inspection of encrypted traffic is not enabled. You must configure a TLS proxy to inspect encrypted traffic.

Configure a Skinny (SCCP) Inspection Policy Map

To specify actions when a message violates a parameter, create an SCCP inspection policy map. You can then apply the inspection policy map when you enable SCCP inspection.

Procedure

Step 1 Create an SCCP inspection policy map: `policy-map type inspect skinny policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2 (Optional) Add a description to the policy map: `description string`

Step 3 (Optional) Drop traffic based on the station message ID field in SCCP messages.

a) Identify the traffic based on the station message ID value in hexadecimal, from 0x0 to 0xffff. You can either specify a single ID, or a range of IDs, using the `match [not] message-id` command. If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

```
match message-id {value | range start_value end_value}
```

Example:

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

b) Specify the action to perform on matching packets. You can drop the packet and optionally log it: `drop [log]`

c) Repeat the process until you identify all message IDs that you want to drop.

Step 4 Configure parameters that affect the inspection engine.

a) Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option:
• **enforce-registration**—Enforces registration before calls can be placed.

• **message-ID max \*hex_value**—Sets the maximum SCCP station message ID allowed. The message ID is in hex, and the default maximum is 0x181.

• **rtp-conformance [enforce-payloadtype]**—Checks RTP packets flowing on the pinholes for protocol conformance. The optional enforce-payloadtype keyword enforces the payload type to be audio or video based on the signaling exchange.

• **sccp-prefix-len \{max | min\} length**—Sets the maximum or minimum SCCP prefix length value allowed. Enter the command twice to set both a minimum and maximum value. The default minimum is 4, there is no default maximum.

• **timeout \{media | signaling\} time**—Sets the timeouts for media and signaling connections (in hh:mm:ss format). To have no timeout, specify 0 for the number. The default media timeout is 5 minutes, the default signaling timeout is one hour.

---

**Example**

The following example shows how to define an SCCP inspection policy map.

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

**What to do next**

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection, on page 315.

### STUN Inspection

Session Traversal Utilities for NAT (STUN), defined in RFC 5389, is used by WebRTC clients for browser-based real-time communications so that plug-ins are not necessary. WebRTC clients often use cloud STUN servers to learn their public IP addresses and ports. WebRTC uses Interactive Connectivity Establishment (ICE, RFC 5245) to verify connectivity between clients. These clients typically use UDP, although they can also use TCP or other protocols.

Because firewalls often block outgoing UDP traffic, WebRTC products such as Cisco Spark can have problems completing connections. STUN inspection opens pinholes for STUN endpoints, and enforces basic STUN and ICE compliance, to allow communications for clients if the connectivity check is acknowledged by both sides. Thus, you can avoid opening new ports in your access rules to enable these applications.
When you enable STUN inspection on the default inspection class, TCP/UDP port 3478 is watched for STUN traffic. The inspection supports IPv4 addresses and TCP/UDP only.

There are some NAT limitations for STUN inspection. For WebRTC traffic, static NAT/PAT44 are supported. Cisco Spark can support additional types of NAT, because Spark does not require pinholes. You can also use NAT/PAT64, including dynamic NAT/PAT, with Cisco Spark.

STUN inspection is supported in failover and cluster modes, as pinholes are replicated. However, the transaction ID is not replicated among units. In the case where a unit fails after receiving a STUN Request and another unit received the STUN Response, the STUN Response will be dropped.

For information on enabling STUN inspection, see Configure Application Layer Protocol Inspection, on page 315.

### History for Voice and Video Protocol Inspection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP, SCCP, and TLS Proxy support for IPv6</td>
<td>9.3(1)</td>
<td>You can now inspect IPv6 traffic when using SIP, SCCP, and TLS Proxy (using SIP or SCCP). We did not modify any commands.</td>
</tr>
<tr>
<td>SIP support for Trust Verification Services, NAT66, CUCM 10.5, and model 8831 phones.</td>
<td>9.3(2)</td>
<td>You can now configure Trust Verification Services servers in SIP inspection. You can also use NAT66. SIP inspection has been tested with CUCM 10.5. We added the trust-verification-server parameter command.</td>
</tr>
<tr>
<td>Improved SIP inspection performance on multiple core ASA.</td>
<td>9.4(1)</td>
<td>If you have multiple SIP signaling flows going through an ASA with multiple cores, SIP inspection performance has been improved. However, you will not see improved performance if you are using a TLS, phone, or IME proxy. We did not modify any commands.</td>
</tr>
<tr>
<td>SIP inspection support in ASA clustering</td>
<td>9.4(1)</td>
<td>You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported. We introduced the following command: show cluster service-policy.</td>
</tr>
<tr>
<td>SIP inspection support for Phone Proxy and UC-IME Proxy was removed.</td>
<td>9.4(1)</td>
<td>You can no longer use Phone Proxy or UC-IME Proxy when configuring SIP inspection. Use TLS Proxy to inspect encrypted traffic. We removed the following commands: phone-proxy, uc-ime. We removed the phone-proxy and uc-ime keywords from the inspect sip command.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>H.323 inspection support for the H.255 FACILITY message coming before the H.225 SETUP message for H.460.18 compatibility.</td>
<td>9.6(1)</td>
<td>You can now configure an H.323 inspection policy map to allow for H.225 FACILITY messages to come before the H.225 SETUP message, which can happen when endpoints comply with H.460.18. We introduced the following command: <strong>early-message</strong>.</td>
</tr>
<tr>
<td>Session Traversal Utilities for NAT (STUN) inspection.</td>
<td>9.6(2)</td>
<td>You can now inspect STUN traffic for WebRTC applications including Cisco Spark. Inspection opens pinholes required for return traffic. We added or modified the following commands: <strong>inspect stun</strong>, <strong>show asp drop</strong>, <strong>show conn detail</strong>, <strong>show service-policy inspect stun</strong>.</td>
</tr>
<tr>
<td>Support for TLSv1.2 in TLS proxy and Cisco Unified Communications Manager 10.5.2.</td>
<td>9.7(1)</td>
<td>You can now use TLSv1.2 with TLS proxy for encrypted SIP or SCCP inspection with the Cisco Unified Communications Manager 10.5.2. The TLS proxy supports the additional TLSv1.2 cipher suites added as part of the <strong>client cipher-suite</strong> command. We modified the following commands: <strong>client cipher-suite</strong>.</td>
</tr>
</tbody>
</table>
CHAPTER 17

Inspection for Mobile Networks

The following topics explain application inspection for protocols used in mobile networks such as LTE. These inspections require the Carrier license. For information on why you need to use inspection for certain protocols, and the overall methods for applying inspection, see Getting Started with Application Layer Protocol Inspection, on page 307.

- Mobile Network Inspection Overview, on page 393
- Licensing for Mobile Network Protocol Inspection, on page 399
- Defaults for GTP Inspection, on page 400
- Configure Mobile Network Inspection, on page 400
- Monitoring Mobile Network Inspection, on page 430
- History for Mobile Network Inspection, on page 434

Mobile Network Inspection Overview

The following topics explain the inspections available for protocols used in mobile networks such as LTE. There are other services available for SCTP traffic in addition to inspection.

GTP Inspection Overview

GPRS Tunneling Protocol is used in GSM, UMTS and LTE networks for general packet radio service (GPRS) traffic. GTP provides a tunnel control and management protocol to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP also uses a tunneling mechanism for carrying user data packets.

Service provider networks use GTP to tunnel multi-protocol packets through the GPRS backbone between endpoints. In GTPv0-1, GTP is used for signaling between gateway GPRS support nodes (GGSN) and serving GPRS support nodes (SGSN). In GTPv2, the signaling is between Packet Data Network Gateways (PGW) and the Serving Gateway (SGW) as well as other endpoints. The GGSN/PGW is the interface between the GPRS wireless data network and other networks. The SGSN/SGW performs mobility, data session management, and data compression.

You can use the ASA to provide protection against rogue roaming partners. Place the device between the home GGSN/PGW and visited SGSN/SGW endpoints and use GTP inspection on the traffic. GTP inspection works only on traffic between these endpoints. In GTPv2, this is known as the S5/S8 interface.

GTP and associated standards are defined by 3GPP (3rd Generation Partnership Project). For detailed information, see http://www.3gpp.org.
GTP Inspection Limitations

Following are some limitations on GTP inspection:

• GTPv2 piggybacking messages are not supported. They are always dropped.

• GTPv2 emergency UE attach is supported only if it contains IMSI (International Mobile Subscriber Identity).

• GTP inspection does not inspect early data. That is, data sent from a PGW or SGW right after a Create Session Request but before the Create Session Response.

• For GTPv2, inspection supports up to 3GPP 29.274 Release 10 version 13. For GTPv0/v1, support is up to release 9 of 3GPP 29.060.

• GTP inspection does not support inter-SGSN handoff to the secondary PDP context. Inspection needs to do the handoff for both primary and secondary PDP contexts.

Stream Control Transmission Protocol (SCTP) Inspection and Access Control

SCTP (Stream Control Transmission Protocol) is described in RFC 4960. The protocol supports the telephony signaling protocol SS7 over IP and is also a transport protocol for several interfaces in the 4G LTE mobile network architecture.

SCTP is a transport-layer protocol operating on top of IP in the protocol stack, similar to TCP and UDP. However, SCTP creates a logical communication channel, called an association, between two end nodes over one or more source or destination IP addresses. This is called multi-homing. An association defines a set of IP addresses on each node (source and destination) and a port on each node. Any IP address in the set can be used as either a source or a destination IP address of data packets associated to this association to form multiple connections. Within each connection, multiple streams may exist to send messages. A stream in SCTP represents a logical application data channel.

The following figure illustrates the relationship between an association and its streams.

*Figure 52: Relationship Between SCTP Association and Streams*

If you have SCTP traffic going through the ASA, you can control access based on SCTP ports, and implement application layer inspection to enable connections and to optionally filter on payload protocol ID to selectively drop, log, or rate limit applications.
Each node can have up to three IP addresses. Any addresses over the limit of three are ignored and not included in the association. Pinholes for secondary IP addresses are opened automatically. You do not need to write access control rules to allow them.

The following sections describe the services available for SCTP traffic in more detail.

**SCTP Stateful Inspection**

Similar to TCP, SCTP traffic is automatically inspected at layer 4 to ensure well-structured traffic and limited RFC 4960 enforcement. The following protocol elements are inspected and enforced:

- Chunk types, flags, and length.
- Verification tags.
- Source and destination ports, to prevent association redirect attacks.
- IP addresses.

SCTP stateful inspection accepts or rejects packets based on the association state:

- Validating the 4-way open and close sequences for initial association establishment.
- Verifying the forward progression of TSN within an association and a stream.
- Terminating an association when seeing the ABORT chunk due to heartbeat failure. SCTP endpoints might send the ABORT chunk in response to bombing attacks.

If you decide you do not want these enforcement checks, you can configure SCTP state bypass for specific traffic classes, as explained in Configure Connection Settings for Specific Traffic Classes (All Services), on page 457.

**SCTP Access Control**

You can create access rules for SCTP traffic. These rules are similar to TCP/UDP port-based rules, where you simply use `sctp` as the protocol, and the port numbers are SCTP ports. You can create service objects or groups for SCTP, or specify the ports directly. See the following topics.

- Configure Service Objects and Service Groups, on page 12
- Add an Extended ACE for Port-Based Matching, on page 29

**SCTP NAT**

You can apply static network object NAT to the addresses in SCTP association establishment messages. Although you can configure static twice NAT, this is not recommended because the topology of the destination part of the SCTP association is unknown. You cannot use dynamic NAT/PAT.

NAT for SCTP depends upon SCTP stateful inspection rather than SCTP application-layer inspection. Thus, you cannot NAT traffic if you configure SCTP state bypass.
SCTP Application Layer Inspection

You can further refine your access rules by enabling SCTP inspection and filtering on SCTP applications. You can selectively drop, log, or rate limit SCTP traffic classes based on the payload protocol identifier (PPID).

If you decide to filter on PPID, keep the following in mind:

- PPIDs are in data chunks, and a given packet can have multiple data chunks or even a control chunk. If a packet includes a control chunk or multiple data chunks, the packet will not be dropped even if the assigned action is drop.

- If you use PPID filtering to drop or rate-limit packets, be aware that the transmitter will resend any dropped packets. Although a packet for a rate-limited PPID might make it through on the next attempt, a packet for a dropped PPID will again be dropped. You might want to evaluate the eventual consequence of these repeated drops on your network.

SCTP Limitations

SCTP support includes the following limitations.

- Each node can have up to three IP addresses. Any addresses over the limit of three are ignored and not included in the association. Pinholes for secondary IP addresses are opened automatically. You do not need to write access control rules to allow them.

- Unused pinholes time out in 5 minutes.

- Dual stack IPv4 and IPv6 addresses on multi-homed endpoints is not supported.

- Network object static NAT is the only supported type of NAT. Also, NAT46 and NAT64 are not supported.

- Fragmentation and reassembly of SCTP packets is done only for traffic handled by Diameter, M3UA, and SCTP PPID-based inspection.

- ASCONF chunks, which are used to dynamically add or delete IP addresses in SCTP, are not supported.

- The Hostname parameter in INIT and INIT-ACK SCTP messages, which is used to specify a hostname which can then be resolved to an IP address, is not supported.

- SCTP/M3UA does not support equal-cost multipath routing (ECMP), whether configured on the ASA or elsewhere in the network. With ECMP, packets can be routed to a destination over multiple best paths. However, an SCTP/M3UA packet response to a single destination has to come back on the same interface that it exited. Even though the response can come from any M3UA server, it must always come back on the same interface that it exited. The symptom for this problem is that SCTP INIT-ACK packets are dropped, which you can see in the show asp drop flow sctp-chunk-init-timeout counter:

  Flow drop:
  SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)

If you encounter this problem, you can resolve it by configuring static routes to the M3UA servers, or by configuring policy-based routing to implement a network design that ensures that INIT-ACK packets go through the same interface as the INIT packets.
Diameter Inspection

Diameter is an Authentication, Authorization, and Accounting (AAA) protocol used in next-generation mobile and fixed telecom networks such as EPS (Evolved Packet System) for LTE (Long Term Evolution) and IMS (IP Multimedia Subsystem). It replaces RADIUS and TACACS in these networks.

Diameter uses TCP and SCTP as the transport layer, and secures communications using TCP/TLS and SCTP/DTLS. It can optionally provide data object encryption as well. For detailed information on Diameter, see RFC 6733.

Diameter applications perform service management tasks such as deciding user access, service authorization, quality of service, and rate of charging. Although Diameter applications can appear on many different control-plane interfaces in the LTE architecture, the ASA inspects Diameter command codes and attribute-value pairs (AVP) for the following interfaces only:

- S6a: Mobility Management Entity (MME) - Home Subscription Service (HSS).
- S9: PDN Gateway (PDG) - 3GPP AAA Proxy/Server.
- Rx: Policy Charging Rules Function (PCRF) - Call Session Control Function (CSCF).

Diameter inspection opens pinholes for Diameter endpoints to allow communication. The inspection supports 3GPP version 12 and is RFC 6733 compliant. You can use it for TCP/TLS (by specifying a TLS proxy when you enable inspection) and SCTP, but not SCTP/DTLS. Use IPsec to provide security to SCTP Diameter sessions.

You can optionally use a Diameter inspection policy map to filter traffic based on application ID, command codes, and AVP, to apply special actions such as dropping packets or connections, or logging them. You can create custom AVP for newly-registered Diameter applications. Filtering lets you fine-tune the traffic you allow on your network.

Note

Diameter messages for applications that run on other interfaces will be allowed and passed through by default. However, you can configure a Diameter inspection policy map to drop these applications by application ID, although you cannot specify actions based on the command codes or AVP for these unsupported applications.

M3UA Inspection

MTP3 User Adaptation (M3UA) is a client/server protocol that provides a gateway to the SS7 network for IP-based applications that interface with the SS7 Message Transfer Part 3 (MTP3) layer. M3UA makes it possible to run the SS7 User Parts (such as ISUP) over an IP network. M3UA is defined in RFC 4666.

M3UA uses SCTP as the transport layer. SCTP port 2905 is the default port.

The MTP3 layer provides networking functions such as routing and node addressing, but uses point codes to identify nodes. The M3UA layer exchanges Originating Point Codes (OPC) and Destination Point Codes (DPC). This is similar to how IP uses IP addresses to identify nodes.

M3UA inspection provides limited protocol conformance. You can optionally implement strict application server process (ASP) state checking and additional message validation for select messages. Strict ASP state checking is required if you want stateful failover or if you want to operate within a cluster. However, strict ASP state checking works in Override mode only, it does not work if you are running in Loadsharing or Broadcast mode (per RFC 4666). The inspection assumes there is one and only one ASP per endpoint.
You can optionally apply access policy based on point codes or Service Indicators (SI). You can also apply rate limiting based on message class and type.

**M3UA Protocol Conformance**

M3UA inspection provides the following limited protocol enforcement. Inspection drops and logs packets that do not meet requirements.

- **Common message header.** Inspection validates all fields in the common header.
  - Version 1 only.
  - Message length must be correct.
  - Message type class with a reserved value is not allowed.
  - Invalid message ID within the message class is not allowed.

- **Payload data message.**
  - Only one parameter of a given type is allowed.
  - Data messages on SCTP stream 0 are not allowed.

- The Affected Point Code field must be present in the following messages or the message is dropped: Destination Available (DAVA), Destination Unavailable (DUNA), Destination State Audit (DAUD), Signaling Congestion (SCON), Destination User Part Unavailable (DUPU), Destination Restricted (DRST).

- If you enable message tag validation for the following messages, the content of certain fields are checked and validated. Messages that fail validation are dropped.
  - Destination User Part Unavailable (DUPU)—The User/Cause field must be present, and it must contain only valid cause and user codes.
  - Error—All mandatory fields must be present and contain only allowed values. Each error message must contain the required fields for that error code.
  - Notify—The status type and status information fields must contain allowed values only.

- If you enable strict application server process (ASP) state validation, the system maintains the ASP states of M3UA sessions and allows or drops ASP messages based on the validation result. If you do not enable strict ASP state validation, all ASP messages are forwarded uninspected.

**M3UA Inspection Limitations**

Following are some limitations on M3UA inspection.

- NAT is not supported for IP addresses that are embedded in M3UA data.

- M3UA strict application server process (ASP) state validation depends on SCTP stateful inspection. Do not implement SCTP state bypass and M3UA strict ASP validation on the same traffic.

- Strict ASP state checking is required if you want stateful failover or if you want to operate within a cluster. However, strict ASP state checking works in Override mode only, it does not work if you are running in Loadsharing or Broadcast mode (per RFC 4666). The inspection assumes there is one and only one ASP per endpoint.
RADIUS Accounting Inspection Overview

The purpose of RADIUS accounting inspection is to prevent over-billing attacks on GPRS networks that use RADIUS servers. Although you do not need the Carrier license to implement RADIUS accounting inspection, it has no purpose unless you are implementing GTP inspection and you have a GPRS setup.

The over-billing attack in GPRS networks results in consumers 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 by ensuring the traffic seen by the GGSN is legitimate. With the RADIUS accounting feature properly configured, the ASA 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 ASA 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 ASA can validate the message. If the shared secret is not configured, the ASA will only check that the source IP address is one of the configured addresses allowed to send the RADIUS messages.

Note

When using RADIUS accounting inspection with GPRS enabled, the ASA checks for the 3GPP-Session-Stop-Indicator in the Accounting Request STOP messages to properly handle secondary PDP contexts. Specifically, the ASA requires that the Accounting Request STOP messages include the 3GPP-SGSN-Address attribute before it will terminate the user sessions and all associated connections. Some third-party GGSNs might not send this attribute by default.

Licensing for Mobile Network Protocol Inspection

Inspection of the following protocols requires the license listed in the table below.

- GTP
- SCTP
- Diameter
- M3UA

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5525-X</td>
<td>Carrier license</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td></td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td></td>
</tr>
<tr>
<td>ASA 5585-X</td>
<td></td>
</tr>
<tr>
<td>ASASM</td>
<td></td>
</tr>
</tbody>
</table>
Defaults for GTP Inspection

GTP inspection is not enabled by default. However, if you enable it without specifying your own inspection map, a default map is used that provides the following processing. You need to configure a map only if you want different values.

- Errors are not permitted.
- The maximum number of requests is 200.
- The maximum number of tunnels is 500. This is equivalent to the number of PDP contexts (endpoints).
- The GTP endpoint timeout is 30 minutes. Endpoints include GSNs (GTPv0,1) and SGW/PGW (GTPv2).
- The PDP context timeout is 30 minutes. In GTPv2, this is the bearer context timeout.
- The request timeout is 1 minute.
- The signaling timeout is 30 minutes.
- The tunneling timeout is 1 hour.
- The T3 response timeout is 20 seconds.
- Unknown message IDs are dropped and logged. This behavior is confined to messages the 3GPP defines for the SS7S interface. Messages defined for other GPRS interfaces might be allowed with minimal inspection.

Messages are considered unknown if they are either undefined or are defined in GTP releases that the system does not support. Supported releases are GTPv1 release 6.1 and GTPv2 release 10.13.

Configure Mobile Network Inspection

Inspections for protocols used in mobile networks are not enabled by default. You must configure them if you want to support mobile networks.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>(Optional.) Configure a GTP Inspection Policy Map, on page 401.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>(Optional.) Configure an SCTP Inspection Policy Map, on page 405.</td>
</tr>
</tbody>
</table>
Step 3  (Optional.) Configure a Diameter Inspection Policy Map, on page 406.
If you want to filter on attribute-value pairs (AVP) that are not yet supported in the software, you can create
custom AVP for use in the Diameter inspection policy map. See Create a Custom Diameter Attribute-Value
Pair (AVP), on page 410.
Step 4  (Optional.) If you want to inspect encrypted Diameter TCP/TLS traffic, create the required TLS proxy as
described in Inspecting Encrypted Diameter Sessions, on page 411
Step 5  (Optional.) Configure an M3UA Inspection Policy Map, on page 422
Step 6  Configure the Mobile Network Inspection Service Policy, on page 425.
Step 7  (Optional.) Configure RADIUS Accounting Inspection, on page 427.
RADIUS accounting inspection protects against over-billing attacks.

Configure a GTP Inspection Policy Map

If you want to enforce additional parameters on GTP traffic, and the default map does not meet your needs,
create and configure a GTP map.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of
those techniques, first create the regular expression or regular expression class map.

Procedure

Step 1  Create a GTP inspection policy map: policy-map type inspect gtp policy_map_name
Where the policy_map_name is the name of the policy map. The CLI enters policy-map configuration mode.
Step 2  (Optional) Add a description to the policy map: description string
Step 3  To apply actions to matching traffic, perform the following steps.
   a) Specify the traffic on which you want to perform actions using one of the following match commands.
      If you use a match not command, then any traffic that does not match the criterion in the match not
command has the action applied.
         • match [not] apn regex {regex_name | class class_name}—Matches the access point name (APN)
against the specified regular expression or regular expression class.
         • match [not] message {v1 | v2} id {message_id | range message_id_1 message_id_2}—Matches
the message ID, which can be 1 to 255. You can specify a single ID or a range of IDs. You must
specify whether the message is for GTPv0/1 (v1) or GTPv2 (v2).
         • match [not] message length min bytes max bytes—Matches messages where the length of the UDP
payload (GTP header plus the rest of the message) is between the minimum and maximum values,
from 1 to 65536.
         • match [not] misisdn regex {regex_name | class class_name}—Matches the Mobile Station
International Subscriber Directory Number (MSISDN) information element in the Create PDP Context
request, Create session request, and Modify Bearer Response messages against the specified regular
expression or regular expression class. The regular expression can identify a specific MSISDN, or a range of MSISDNs based on the first x number of digits. MSISDN filtering is supported for GTPv1 and GTPv2 only.

- **match [not] selection-mode mode_value**—Matches the Selection Mode information element in the Create PDP Context request. The selection mode specifies the origin of the Access Point Name (APN) in the message, and can be one of the following. Selection Mode filtering is supported for GTPv1 and GTPv2 only.
  - 0—Verified. The APN was provided by the mobile station or network, and the subscription is verified.
  - 1—Mobile Station. The APN was provided by the mobile station, and the subscription is not verified.
  - 2—Network. The APN was provided by the network, and the subscription is not verified.
  - 3—Reserved, not used.

- **match [not] version {version_id | range version_id_1 version_id_2}**—Matches the GTP version, which can be 0 to 255. You can specify a single version or a range of versions.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:

- **drop [log]**—Drop all packets that match. Add the log keyword to also send a system log message.
- **rate-limit message_rate**—Limit the rate of messages. This option is available with **message_id** only.

You can specify multiple **match** commands in the policy map. For information about the order of **match** commands, see *How Multiple Traffic Classes are Handled*, on page 308.

**Step 4**

To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option:

- **anti-replay [window_size]**—Enable anti-replay by specifying a sliding window for GTP-U messages. The size of the sliding window is in number of messages and can be 128, 256, 512, or 1024. If you do not specify a size, you get the default, 512. As valid messages appear, the window moves to the new sequence numbers. Sequence numbers are in the range 0-65535, wrapping when they reach the maximum, and they are unique per PDP context. Messages are considered valid if their sequence numbers are within the window. Anti-replay helps prevent session hijacking or DoS attacks, which can occur when a hacker captures GTP data packets and replays them.

- **permit errors**—Allows invalid GTP packets or packets that otherwise would fail parsing and be dropped.

- **request-queue max_requests**—Sets the maximum number of GTP requests that will be queued waiting for a response. The default is 200. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the
Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

- **tunnel-limit max_tunnels**—Sets the maximum number of active GTP tunnels allowed. This is equivalent to the number of PDP contexts or endpoints. The default is 500. New requests will be dropped once the number of tunnels specified by this command is reached.

- **timeout** {endpoint | pdp-context | request | signaling | t3-response | tunnel} time—Sets the idle timeout for the specified service (in hh:mm:ss format). To have no timeout, specify 0 for the number. Enter the command separately for each timeout.
  - **endpoint**—The maximum period of inactivity before a GTP endpoint is removed.
  - **pdp-context**—The maximum period of inactivity before removing the PDP Context for a GTP session. In GTPv2, this is the bearer context.
  - **request**—The maximum period of inactivity after which a request is removed from the request queue. Any subsequent responses to a dropped request will also be dropped.
  - **signaling**—The maximum period of inactivity before GTP signaling is removed.
  - **t3-response**—The maximum wait time for a response before removing the connection.
  - **tunnel**—The maximum period of inactivity for the GTP tunnel before it is torn down.

**Step 5** While still in parameter configuration mode, configure GTP-U checking for IP packets and anti-spoofing.

```plaintext
gtp-u-header-check [anti-spoofing [gtpv2-dhcp-bypass | gtpv2-dhcp-drop]]
```

Without keywords, this command checks whether the inner payload of a GTP data packet is a valid IP packet, and drops the packet if it has a non-IP header.

If you include the **anti-spoofing** keyword, the system also checks whether the mobile user IP address in the IP header of the inner payload matches the IP address assigned in GTP control messages such as Create Session Response, and drops the GTP-U message if the IP addresses do not match. This check supports IPv4, IPv6, and IPv4v6 PDN Types. If the mobile station gets its address using DHCP, the end-user IP address in GTPv2 is 0.0.0.0 (IPv4) or prefix::0 (IPv6), so in this case, the system updates the end-user IP address with the first IP address found in the inner packets. You can change the default behavior for DHCP-obtained addresses using the following keywords:

- **gtpv2-dhcp-bypass**—Do not update the 0.0.0.0 or prefix::0 address. Instead, allow packets where the end-user IP address is 0.0.0.0 or prefix::0. This option bypasses the anti-spoofing check when DHCP is used to obtain the IP address.

- **gtpv2-dhcp-drop**—Do not update the 0.0.0.0 or prefix::0 address. Instead, drop all packets where the end-user IP address is 0.0.0.0 or prefix::0. This option prevents access for users that use DHCP to obtain the IP address.

**Step 6** While still in parameter configuration mode, configure IMSI prefix filtering, if desired:

```plaintext
mcc country_code mnc network_code
```

By default, GTP inspection does not check for valid Mobile Country Code (MCC)/Mobile Network Code (MNC) combinations. If you configure IMSI prefix filtering, the MCC and MNC in the IMSI of the received packet is compared with the configured MCC/MNC combinations and is dropped if it does not match.
The Mobile Country Code is a non-zero, three-digit value; add zeros as a prefix for one- or two-digit values. The Mobile Network Code is a two- or three-digit value.

Add all permitted MCC and MNC combinations. By default, the ASA does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

**Step 7** While still in parameter configuration mode, configure GSN or PGW pooling, if desired.

```plaintext
permit-response to-object-group SGSN-SGW_name from-object-group GSN-PGW_pool
```

When the ASA performs GTP inspection, by default the ASA drops GTP responses from GSNs or PGWs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs or PGWs to provide efficiency and scalability of GPRS.

To configure GSN/PGW pooling and thus support load balancing, create a network object group that specifies the GSN/PGW endpoints and specify this on the `from-object-group` parameter. Likewise, create a network object group for the SGSN/SGW and select it on the `to-object-group` parameter. If the GSN/PGW responding belongs to the same object group as the GSN/PGW that the GTP request was sent to and if the SGSN/SGW is in an object group that the responding GSN/PGW is permitted to send a GTP response to, the ASA permits the response.

The network object group can identify the endpoints by host address or by the subnet that contains them.

**Example:**

The following is an example of GSN/PGW pooling. An entire Class C network is defined as the GSN/PGW pool but you can identify multiple individual IP addresses, one per `network-object` command, instead of identifying whole networks. The example then modifies a GTP inspection map to permit responses from the pool to the SGSN/SGW.

```plaintext
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

**Example**

The following example shows how to limit the number of tunnels in the network:

```plaintext
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap
```
Configure an SCTP Inspection Policy Map

To apply alternative actions to SCTP traffic based on the application-specific payload protocol identifier (PPID), such as rate limiting, create an SCTP inspection policy map to be used by the service policy.

Note

PPIDs are in data chunks, and a given packet can have multiple data chunks or even a control chunk. If a packet includes a control chunk or multiple data chunks, the packet will not be dropped even if the assigned action is drop. For example, if you configure an SCTP inspection policy map to drop PPID 26, and a PPID 26 data chunk is combined in a packet with a Diameter PPID data chunk, that packet will not be dropped.

Procedure

Step 1
Create an SCTP inspection policy map: `policy-map type inspect sctp policy_map_name`
Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2
(Optional) Add a description to the policy map: `description string`

Step 3
Drop, rate limit, or log traffic based on the PPID in SCTP data chunks.

a) Identify the traffic based on the PPID.

```
match [not] ppid ppid_1 [ppid_2]
```

Where `ppid_1` is the PPID number (0-4294967295) or name (see the CLI help for the available names). You can include a second (higher) PPID, `ppid_2`, to specify a range of PPIDs. Use `match not ppid` to identify traffic that does not match the PPID or range.


b) Specify the action to perform on matching packets.

- **drop**—Drop and log all packets that match.
- **log**—Send a system log message.
- **rate-limit rate**—Limit the rate of messages. The rate is in kilobits per second (kbps).

c) Repeat the process until you identify all PPIDs you want to selectively handle.
Example
The following example creates an inspection policy map that will drop unassigned PPIDs (unassigned at the time this example was written), rate limit PPIDs 32-40, and log the Diameter PPID. The service policy applies the inspection to the inspection_default class, which matches all SCTP traffic.

```
policy-map type inspect sctp sctp-pmap
  match ppid 58 4294967295
    drop
  match ppid 26
    drop
  match ppid 49
    drop
  match ppid 32 40
    rate-limit 1000
  match ppid diameter
    log

policy-map global_policy
  class inspection_default
    inspect sctp sctp-pmap
      service-policy global_policy global
```

What to do next
You can now configure an inspection policy to use the map. See Configure the Mobile Network Inspection Service Policy, on page 425.

Configure a Diameter Inspection Policy Map
You can create a Diameter inspection policy map to filter on various Diameter protocol elements. You can then selectively drop or log connections.

To configure Diameter message filtering, you must have a good knowledge of these protocol elements as they are defined in RFCs and technical specifications. For example, the IETF has a list of registered applications, command codes, and attribute-value pairs at 
http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml, although Diameter inspection does not support all listed items. See the 3GPP web site for their technical specifications.

Before you begin
Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

Procedure

**Step 1** (Optional) Create a Diameter inspection class map by performing the following steps.

A class map groups multiple traffic matches. You can alternatively identify `match` commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.
To specify traffic that should not match the class map, use the `match not` command. For example, if the `match not` command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you specify actions to take on the traffic in the inspection policy map.

If you want to perform different actions for each `match` command, you should identify the traffic directly in the policy map.

a) Create the class map: `class-map type inspect diameter [match-all | match-any] class_map_name`
   Where `class_map_name` is the name of the class map. The `match-all` keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one `match` statement. The CLI enters class-map configuration mode, where you can enter one or more `match` commands.

b) (Optional) Add a description to the class map: `description string`
   Where `string` is the description of the class map (up to 200 characters).

c) Specify the traffic on which you want to perform actions using one of the following `match` commands.
   If you use a `match not` command, then any traffic that does not match the criterion in the `match not` command has the action applied.

   • `match [not] application-id app_id [app_id_2]`—Matches the application identifier, where `app_id` is the Diameter application name or number (0-4294967295). If there is a range of consecutively-numbered applications that you want to match, you can include a second ID. You can define the range by application name or number, and it applies to all the numbers between the first and second IDs.

   These applications are registered with the IANA. Following are the core supported applications, but you can filter on other applications. Use the CLI help for a list of application names.

   • `3gpp-rx-ts29214` (16777236)
   • `3gpp-s6a` (16777251)
   • `3gpp-s9` (16777267)
   • `common-message` (0). This is the base Diameter protocol.

   • `match [not] command-code code [code_2]`—Matches the command code, where `code` is the Diameter command code name or number (0-4294967295). If there is a range of consecutively-numbered command codes that you want to match, you can include a second code. You can define the range by command code name or number, and it applies to all the numbers between the first and second codes.

   For example, the following command matches the Capability Exchange Request/Answer command code:

   ```
   match command-code cer-cea
   ```

   • Match the attribute-value pair (AVP).

   To match AVP by attribute only:

   ```
   match [not] avp code [code_2] [vendor-id id_number]
   ```
To match an AVP based on the value of the attribute:

```
match [not] avp code [vendor-id id_number] value
```

Where:

- **code**—The name or number (1-4294967295) of an attribute-value pair. For the first code, you can specify the name of a custom AVP or one that is registered in RFCs or 3GPP technical specifications and is directly supported in the software. If you want to match a range of AVP, specify the second code by number only. If you want to match an AVP by its value, you cannot specify a second code. See the CLI help for a list of AVP names.

- **vendor-id id_number**—(Optional.) The ID number of the vendor to also match, from 0-4294967295. For example, the 3GPP vendor ID is 10415, the IETF is 0.

- **value**—The value portion of the AVP. You can configure this only if the data type of the AVP is supported. For example, you can specify an IP address for AVP that have the address data type. Following are the specific syntax of the value option for the supported data types:

  - **Diameter Identity, Diameter URI, Octet String**—Use regular expression or regular expression class objects to match these data types.
    
    ```
    {regex regex_name | class regex_class}
    ```

  - **Address**—Specify the IPv4 or IPv6 address to match. For example, 10.100.10.10 or 2001:DB8::0DB8:800:200C:417A.

  - **Time**—Specify the start and end dates and time. Both are required. Time is in 24-hour format.

    ```
    date year month day time hh:mm:ss date year month day time hh:mm:ss
    ```

    For example:

    ```
    date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00
    ```

  - **Numeric**—Specify a range of numbers:

    ```
    range number_1 number_2
    ```

    The valid number range depends on the data type:

    - **Integer32**—-2147483647 to 2147483647
    - **Integer64**—-9223372036854775807 to 9223372036854775807
    - **Unsigned32**—0 to 4294967295
    - **Unsigned64**—0 to 18446744073709551615
    - **Float32**—decimal point representation with 8 digit precision
    - **Float64**—decimal point representation with 16 digit precision

     d) Enter **exit** to leave class map configuration mode.

**Step 2**

Create a Diameter inspection policy map: `policy-map type inspect diameter policy_map_name`

Where the **policy_map_name** is the name of the policy map. The CLI enters policy-map configuration mode.
Step 3  (Optional) Add a description to the policy map: description string

Step 4  To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following methods:
   • If you created a Diameter class map, specify it by entering the following command: class class_map_name
   • Specify traffic directly in the policy map using one of the match commands described for Diameter class maps.

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:
   • drop—Drop all packets that match.
   • drop-connection—Drop the packet and close the connection.
   • log—Send a system log message.

You can specify multiple class or match commands in the policy map. For information about the order of class and match commands, see How Multiple Traffic Classes are Handled, on page 308.

Example:

hostname(config)# policy-map type inspect diameter diameter-map
hostname(config-pmap)# class diameter-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match command-code cer-cea
hostname(config-pmap-c)# log

Step 5  To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode.

   hostname(config-pmap)# parameters
   hostname(config-pmap-p)#

b) Set one or more parameters. You can set the following options; use the no form of the command to disable the option.

   • unsupported {application-id | command-code | avp} action log—Enables logging for unsupported Diameter elements. These options specify application IDs, command codes, and AVP that are not directly supported by the software. The default is to allow the elements without logging them. You can enter the command three times to enable logging for all elements.

   • strict-diameter {state | session}—Enables strict Diameter protocol conformance to RFC 6733. By default, inspection ensures that Diameter frames comply with the RFC. You can add state machine validation or session-related message validation, or both by entering the command twice.

Example:

hostname(config-pmap)# parameters
hostname(config-pmap-p)# unsupported application-id action log
hostname(config-pmap-p)# unsupported command-code action log
hostname(config-pmap-p)# unsupported avp action log
hostname(config-pmap-p)# strict-diameter state
Example
The following example shows a how to log some applications and block a specific IP address.

class-map type inspect diameter match-any log_app
  match application-id 3gpp-s6a
  match application-id 3gpp-s13

class-map type inspect diameter match-all block_ip
  match command-code cer-cea
  match avp host-ip-address 1.1.1.1

policy-map type inspect diameter diameter_map
  parameters
    unsupported application-id log
  class log_app
    log
  class block_ip
    drop-connection

policy-map global_policy
  class inspection_default
    inspect diameter diameter_map

service-policy global_policy global

What to do next
You can now configure an inspection policy to use the map. See Configure the Mobile Network Inspection Service Policy, on page 425.

Create a Custom Diameter Attribute-Value Pair (AVP)

As new attribute-value pairs (AVP) are defined and registered, you can create custom Diameter AVP to define them and use them in your Diameter inspection policy map. You would get the information you need to create the AVP from the RFC or other source that defines the AVP.

Create custom AVP only if you want to use them in a Diameter inspection policy map or class map for AVP matching.

Procedure

Create a custom Diameter AVP.

diameter avp name code value data-type type [vendor-id id_number] [description text]

Where:
• **name**—The name of the custom AVP you are creating, up to 32 characters. You would refer to this name on the match avp command in a Diameter inspection policy map or class map.

• **code value**—The custom AVP code value, from 256-4294967295. You cannot enter a code and vendor-id combination that is already defined in the system.

• **data-type type**—The data type of the AVP. You can define AVP of the following types. If the new AVP is of a different type, you cannot create a custom AVP for it.
  - **address**—For IP addresses.
  - **diameter-identity**—Diameter identity data.
  - **diameter-uri**—Diameter uniform resource identifier (URI).
  - **float32**—32-bit floating point number.
  - **float64**—64-bit floating point number.
  - **int32**—32-bit integer.
  - **int64**—64-bit integer.
  - **octetstring**—Octet string.
  - **time**—Time value.
  - **uint32**—32-bit unsigned integer.
  - **uint64**—64-bit unsigned integer.

• **vendor-id id number**—(Optional.) The ID number of the vendor who defined the AVP, from 0-4294967295. For example, the 3GPP vendor ID is 10415, the IETF is 0.

• **description text**—(Optional.) A description of the AVP, up to 80 characters. Enclose the description in quotation marks if you include spaces.

---

**Inspecting Encrypted Diameter Sessions**

If a Diameter application uses encrypted data over TCP, inspection cannot see inside the packets to implement your message filtering rules. Thus, if you create filtering rules, and you want them to also apply to encrypted TCP traffic, you must configure a TLS proxy. You also need a proxy if you want strict protocol enforcement on encrypted traffic. This configuration does not apply to SCTP/DTLS traffic.

The TLS proxy acts as a man-in-the-middle. It decrypts traffic, inspects it, then encrypts it again and sends it to the intended destination. Thus, both sides of the connection, the Diameter server and Diameter client, must trust the ASA, and all parties must have the required certificates. You must have a good understanding of digital certificates to implement TLS proxy. Please read the chapter on digital certificates in the ASA general configuration guide.

The following illustration shows the relationship among the Diameter client and server, and the ASA, and the certification requirements to establish trust. In this model, a Diameter client is an MME (Mobility Management Entity), not an end user. The CA certificate on each side of a link is the one used to sign the certificate on the
other side of the link. For example, the ASA proxy TLS server CA certificate is the one used to sign the Diameter/TLS client certificate.

*Figure 53: Diameter TLS Inspection*

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Diameter TLS client (MME)</td>
<td>2</td>
<td>ASA proxy TLS server</td>
</tr>
<tr>
<td></td>
<td>• Client identity certificate</td>
<td></td>
<td>• Server identity certificate</td>
</tr>
<tr>
<td></td>
<td>• CA certificate used to sign the ASA TLS proxy server's identity certificate</td>
<td></td>
<td>• CA certificate used to sign the Diameter TLS client's identity certificate</td>
</tr>
<tr>
<td>3</td>
<td>ASA proxy TLS client</td>
<td>4</td>
<td>Diameter TLS server (full proxy)</td>
</tr>
<tr>
<td></td>
<td>• Client identity (static or LDC) certificate</td>
<td></td>
<td>• Server identity certificate</td>
</tr>
<tr>
<td></td>
<td>• CA certificate used to sign the Diameter TLS server identity certificate</td>
<td></td>
<td>• CA certificate used to sign the ASA proxy TLS client's identity certificate</td>
</tr>
<tr>
<td>5</td>
<td>Diameter TCP server (TLS offload)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You have the following options for configuring TLS proxy for Diameter inspection:

- **Full TLS proxy**—Encrypt traffic between the ASA and Diameter clients and the ASA and Diameter server. You have the following options for establishing the trust relationship with the TLS server:
  - Use a static proxy client trustpoint. The ASA presents the same certificate for every Diameter client when communicating with the Diameter server. Because all clients look the same, the Diameter server cannot provide differential services per client. On the other hand, this option is faster than the LDC method.
  - Use local dynamic certificates (LDC). With this option, the ASA presents unique certificates per Diameter client when communicating with the Diameter server. The LDC retains all fields from the received client identity certificate except its public key and a new signature from the ASA. This method gives the Diameter server better visibility into client traffic, which makes it possible to provide differential services based on client certificate characteristics.

- **TLS offload**—Encrypt traffic between the ASA and Diameter client, but use a clear-text connection between the ASA and Diameter server. This option is viable if the Diameter server is in the same data center as the ASA, where you are certain that the traffic between the devices will not leave the protected area. Using TLS offload can improve performance, because it reduces the amount of encryption processing.
required. It should be the fastest of the options. The Diameter server can apply differential services based on client IP address only.

All three options use the same configuration for the trust relationship between the ASA and Diameter clients.

Note

TLS proxy uses TLSv1.0 - 1.2. You can configure the TLS version and the cipher suite.

The following topics explain how to configure TLS proxy for Diameter inspection.

Configure Server Trust Relationship with Diameter Clients

The ASA acts as a TLS proxy server in relation to the Diameter clients. To establish the mutual trust relationship:

- You need to import the Certificate Authority (CA) certificate used to sign the ASA’s server certificate into the Diameter client. This might be in the client’s CA certificate store or some other location that the client uses. Consult the client documentation for exact details on certificate usage.

- You need to import the CA certificate used to sign the Diameter TLS client’s certificate so the ASA can trust the client.

The following procedure explains how to import the CA certificate used to sign the Diameter client’s certificate, and import an identity certificate to use for the ASA TLS proxy server. Instead of importing an identity certificate, you could create a self-signed certificate on the ASA.

Procedure

Step 1

Import the CA certificate that is used to sign the Diameter client’s certificate into an ASA trustpoint.

This step allows the ASA to trust the Diameter clients.

a) Create the trustpoint for the Diameter client.

In this example, enrollment terminal indicates you will paste the certificate into the CLI. The trustpoint is called diameter-clients.

```
ciscoasa(config)# crypto ca trustpoint diameter-clients
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) Add the certificate.

```
ciscoasa(config)# crypto ca authenticate diameter-clients
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VPUNZzL+JbRTANBgkqhkiG9w0BAQUFBADF
[certificate data omitted]
\7QEMBizyGEOTSEzRu7M6jw5e4qtkQ==
quit

INFO: Certificate has the following attributes:
```
**Step 2** Import the certificate and create a trustpoint for the ASA proxy server’s identity certificate and keypair.

This step allows the Diameter clients to trust the ASA.

a) Import the certificate in pkcs12 format.

   In the following example, **tls-proxy-server-tp** is the trustpoint name and “**123**” is the decryption pass phrase. Use your own trustpoint name and pass phrase.

```plaintext
ciscoasa (config)# crypto ca import tls-proxy-server-tp pkcs12 "123"
```

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:

```plaintext
[PKCS12 data omitted]
quit
```

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#

b) Configure the trustpoint.

```plaintext
ciscoasa(config)# crypto ca trustpoint tls-proxy-server-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

---

**Configure Full TLS Proxy with Static Client Certificate for Diameter Inspection**

If the Diameter server can accept the same certificate for all clients, you can set up a static client certificate for the ASA to use when communicating with the Diameter server.

With this configuration, you need to establish the mutual trust relationship between the ASA and clients (as explained in **Configure Server Trust Relationship with Diameter Clients, on page 413**), and the ASA and Diameter server. Following are the ASA and Diameter server trust requirements.

- You need to import the CA certificate used to sign the Diameter Server's identity certificate so the ASA can validate the server's identity certificate during the TLS handshake.

- You need to import the client certificate, one that the Diameter server also trusts. If the Diameter server does not already trust the certificate, import the CA certificate used to sign it into the server. Consult the Diameter server’s documentation for details.
Procedure

**Step 1** Import the CA certificate that is used to sign the Diameter server’s certificate into an ASA trustpoint. This step allows the ASA to trust the Diameter server.

a) Create the trustpoint for the Diameter server.

   In this example, **enrollment terminal** indicates you will paste the certificate into the CLI. You could also use enrollment url to specify automatic enrollment (SCEP) with the CA. The trustpoint is called **diameter-server**.

   ```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
   ```

b) Add the certificate.

   ```
ciscoasa(config)# crypto ca authenticate diameter-server
   Enter the base 64 encoded CA certificate.
   End with a blank line or the word "quit" on a line by itself
   MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZLzL+JERTANBgkqhkiG9w0BAQUFADCB
   [certificate data omitted]
   /7QEM8izy0zOy7SExRu7Njdj76jwE5e4qtkQ==
   quit
   INFO: Certificate has the following attributes:
   Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
   Do you accept this certificate? [yes/no]: y
   Trustpoint CA certificate accepted.
   % Certificate successfully imported
   ```

**Step 2** Import the certificate and create a trustpoint for the ASA proxy client’s identity certificate and keypair. This step allows the Diameter server to trust the ASA.

a) Import the certificate in pkcs12 format.

   In the following example, **tls-proxy-client-tp** is the trustpoint name and “123” is the decryption pass phrase. Use your own trustpoint name and pass phrase.

   ```
ciscoasa {config}# crypto ca import tls-proxy-client-tp pkcs12 "123"
   Enter the base 64 encoded pkcs12.
   End with a blank line or the word "quit" on a line by itself:
   [PKCS12 data omitted]
   quit
   INFO: Import PKCS12 operation completed successfully
   ```

b) Configure the trustpoint.
ciscoasa(config)# crypto ca trustpoint tls-proxy-client-tp
ciscoasa(ca-trustpoint)# revocation-check none

**Step 3** Configure the TLS proxy.

a) Name the TLS proxy and enter TLS proxy configuration mode.

```
tls-proxy name
```

b) Identify the trustpoint used when the ASA acts as the proxy server in relationship to the Diameter clients.

```
server trust-point trustpoint_name
```

*Note* For testing purposes, or if you are certain that you can trust the Diameter clients, you can skip this step and include the `no server authenticate-client` command in the TLS proxy configuration.

c) Identify the trustpoint used when the ASA acts as the proxy client in relationship to the Diameter server.

```
client trust-point name
```

d) (Optional.) Define the ciphers that the client can use.

```
client cipher-suite cipher-list
```

Where `cipher-list` can include any combination of the following:

- 3des-sha1
- aes128-sha1
- aes256-sha1
- des-sha1
- null-sha1
- rc4-sha1

Separate multiple options with spaces.

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the `ssl cipher` command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the `client cipher-suite` command only if you want to use a different suite than the one generally available on the ASA.

To set the minimum TLS version for all SSL client connections on the ASA, see the `ssl client-version` command. The default is TLS v1.0.

e) (Optional.) Define the ciphers that the server can use.

```
server cipher-suite cipher-list
```

Where `cipher-list` can include any combination of the following:

- 3des-sha1
- aes128-sha1
- aes256-sha1
Separate multiple options with spaces.

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the `ssl cipher` command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the `server cipher-suite` command only if you want to use a different suite than the one generally available on the ASA.

To set the minimum TLS version for all SSL server connections on the ASA, see the `ssl server-version` command. The default is TLS v1.0.

Example:

```plaintext
ciscoasa(config)# tls-proxy diameter-tls-static-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client trust-point tls-proxy-client-tp
```

What to do next

You can now use the TLS proxy in Diameter inspection. See Configure the Mobile Network Inspection Service Policy, on page 425.

Configure Full TLS Proxy with Local Dynamic Certificates for Diameter Inspection

If the Diameter server needs unique certificates for each client, you can configure the ASA to generate local dynamic certificates (LDC). These certificates exist for the duration of the client’s connection and are then destroyed.

With this configuration, you need to establish the mutual trust relationship between the ASA and clients (as explained in Configure Server Trust Relationship with Diameter Clients, on page 413), and the ASA and Diameter server. The configuration is similar to the one described in Configure Full TLS Proxy with Static Client Certificate for Diameter Inspection, on page 414, except instead of importing a Diameter client certificate, you set up the LDC on the ASA. Following are the ASA and Diameter server trust requirements.

- You need to import the CA certificate used to sign the Diameter Server's identity certificate so the ASA can validate the server's identity certificate during the TLS handshake.
- You need to create the LDC trustpoint. You need to export the LDC server’s CA certificate and import it into the Diameter server. The export step is explained below. Consult the Diameter server’s documentation for information on importing certificates.

Procedure

**Step 1** Import the CA certificate that is used to sign the Diameter server’s certificate into an ASA trustpoint.

This step allows the ASA to trust the Diameter server.
Configure Full TLS Proxy with Local Dynamic Certificates for Diameter Inspection

a) Create the trustpoint for the Diameter server.

In this example, enrollment terminal indicates you will paste the certificate into the CLI. You could also use enrollment url to specify automatic enrollment (SCEP) with the CA. The trustpoint is called diameter-server.

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) Add the certificate.

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate. 
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JdRTANBgkqhkiG9w0BAQQDFADCB
[certificate data omitted]
/7QEM8izy0EOT5ErKu7Nd76jwf5e4gttkQ==
quit
INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Step 2

Create the local CA to sign local dynamic certificates (LDC).

a) Create an RSA keypair for the trustpoint.

In this example, the keypair name is ldc-signer-key.

```
ciscoasa(config)# crypto key generate rsa label ldc-signer-key
INFO: The name for the keys will be: ldc-signer-key
Keypair generation process
```

b) Create the LDC issuer trustpoint.

In this example, the trustpoint name is ldc-server, the keypair created above is used, self-signed enrollment is specified (enrollment self, which is required), and the common name of the ASA is included as the subject name. Check whether the Diameter application has specific requirements for the subject name.

The proxy-ldc-issuer command defines the local CA role for the trustpoint to issue dynamic certificates for TLS proxy.

```
ciscoasa(config)# crypto ca trustpoint ldc-server
```

```
ciscoasa(config)# crypto ca trustpoint ldc-server
```

```
ciscoasa(config)# crypto ca trustpoint ldc-server
```

```
ciscoasa(config)# crypto ca trustpoint ldc-server
```

```
ciscoasa(config)# crypto ca trustpoint ldc-server
```

```ciscoasa(config)# crypto ca trustpoint ldc-server
```
Step 3 Configure the TLS proxy.
a) Name the TLS proxy and enter TLS proxy configuration mode.
   \texttt{tls-proxy name}

b) Identify the trustpoint used when the ASA acts as the server in relationship to the Diameter clients.
   \texttt{server trust-point trustpoint_name}

   \textbf{Note} For testing purposes, or if you are certain that you can trust the Diameter clients, you can skip this step and include the \texttt{no server authenticate-client} command in the TLS proxy configuration.

c) Identify the LDC trustpoint used when the ASA issues dynamic certificates and acts as the client in relationship to the Diameter server.
   \texttt{client ldc issuer name}

d) Identify the LDC keypair. Specify the same key that is defined in the LDC trustpoint.
   \texttt{client ldc key-pair name}

e) (Optional.) Define the ciphers that the client can use.
   \texttt{client cipher-suite cipher-list}

   Where \texttt{cipher-list} can include any combination of the following:
   \begin{itemize}
   \item \texttt{3des-sha1}
   \item \texttt{aes128-sha1}
   \item \texttt{aes256-sha1}
   \item \texttt{des-sha1}
   \item \texttt{null-sha1}
   \item \texttt{rc4-sha1}
   \end{itemize}

   Separate multiple options with spaces.

   If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the \texttt{ssl cipher} command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the \texttt{client cipher-suite} command only if you want to use a different suite than the one generally available on the ASA.

   To set the minimum TLS version for all SSL client connections on the ASA, see the \texttt{ssl client-version} command. The default is TLS v1.0.

f) (Optional.) Define the ciphers that the server can use.
   \texttt{server cipher-suite cipher-list}

   Where \texttt{cipher-list} can include any combination of the following:
   \begin{itemize}
   \item \texttt{3des-sha1}
   \end{itemize}
Separate multiple options with spaces.

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the `sslcipher` command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the `serverciphersuite` command only if you want to use a different suite than the one generally available on the ASA.

To set the minimum TLS version for all SSL server connections on the ASA, see the `sslserversversion` command. The default is TLS v1.0.

**Example:**

```
ciscoasa(config)# tls-proxy diameter-tls-ldc-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client ldc issuer ldc-server
ciscoasa(config-tlsp)# client ldc key-pair ldc-signer-key
```

**Step 4**

Export the LDC CA certificate and import it into the Diameter server.

a) Export the certificate.

```plaintext
In the following example, the LDC trustpoint is ldc-server; specify your own LDC trustpoint name.

ciscoasa(config)# crypto ca export ldc-server identity-certificate
-----BEGIN CERTIFICATE-----
MIIDbDCCAlsGAwIBAgIQfWOQyGnPj7hCCB49+ks4CjJANBgkqkig9w0BAQQAdg
MRwYWVVQDWh1dW5ueUJZaAeFw0xMzA2MjUwMTESM2JjQjw0MDTA==
...

-----END CERTIFICATE-----
```

b) Copy the certificate data and save it into a file.

You can now import it into the Diameter server. Consult the Diameter server's documentation for the procedure. Note that the data is in Base64 format. If your server requires binary or DER format, you will need to use OpenSSL tools to convert formats.

**What to do next**

You can now use the TLS proxy in Diameter inspection. See Configure the Mobile Network Inspection Service Policy, on page 425.
Configure TLS Proxy with TLS Offload for Diameter Inspection

If you are certain the network path between the ASA and Diameter server is secure, you can avoid the performance cost of encrypting data between the ASA and server. With TLS offload, the TLS proxy encrypts/decrypts sessions between the Diameter client and the ASA, but uses clear text with the Diameter server.

With this configuration, you need to establish the mutual trust relationship between the ASA and clients only, which simplifies the configuration. Before doing the following procedure, complete the steps in Configure Server Trust Relationship with Diameter Clients, on page 413.

Procedure

**Step 1** Configure the TLS proxy with TLS offload.

a) Name the TLS proxy and enter TLS proxy configuration mode.

```
tls-proxy name
```

b) Identify the trustpoint used when the ASA acts as the server in relationship to the Diameter clients.

```
server trust-point trustpoint_name
```

**Note** For testing purposes, or if you are certain that you can trust the Diameter clients, you can skip this step and include the `no server authenticate-client` command in the TLS proxy configuration.

c) (Optional.) Define the ciphers that the server can use.

```
server cipher-suite cipher-list
```

Where `cipher-list` can include any combination of the following:

- `3des-sha1`
- `aes128-sha1`
- `aes256-sha1`
- `des-sha1`
- `null-sha1`
- `rc4-sha1`

Separate multiple options with spaces.

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the `ssl cipher` command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the `server cipher-suite` command only if you want to use a different suite than the one generally available on the ASA.

To set the minimum TLS version for all SSL server connections on the ASA, see the `ssl server-version` command. The default is TLS v1.0.

d) Specify that communication between the ASA and the Diameter server should be in clear text. In this relationship, the ASA acts as a client of the Diameter server.

```
client clear-text
```
Example:

```cisco
    ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
    ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
    ciscoasa(config-tlsp)# client clear-text
```

Step 2
Because the Diameter ports differ for TCP and TLS, configure a NAT rule to translate the TCP port to the TLS port for traffic going from the Diameter server to the client.

Create an object NAT rule for each Diameter server. Each rule should:

- Perform static identity NAT for the Diameter server address. That is, the IP address in the object should be the same as the translated address in the NAT rule.
- Translate the real port 3868, which is the default Diameter TCP port number, to 5868, the default Diameter TLS port number.
- The source interface should be the one that connects to the Diameter server, and the destination interface the one that connects to the Diameter client.

The following example translates TCP traffic on port 3868 coming to the outside interface from the 10.29.29.29 Diameter server to port 5868 on the inside interface.

```cisco
    ciscoasa(config)# object network diameter-client
    ciscoasa(config-network-object)# host 10.29.29.29
    ciscoasa(config-network-object)# nat (outside,inside) static 10.29.29.29 service tcp 3868 5868
```

What to do next
You can now use the TLS proxy in Diameter inspection. See Configure the Mobile Network Inspection Service Policy, on page 425.

Configure an M3UA Inspection Policy Map

Use an M3UA inspection policy map to configure access control based on point codes. You can also drop and rate limit messages by class and type.

The default point code format is ITU. If you use a different format, specify the required format in the policy map.

If you do not want to apply policy based on point code or message class, you do not need to configure an M3UA policy map. You can enable inspection without a map.

Procedure

Step 1
Create an M3UA inspection policy map: `policy-map type inspect m3ua policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2
(Optional) Add a description to the policy map: `description string`
Step 3 To apply actions to matching traffic, perform the following steps.

a) Specify the traffic on which you want to perform actions using one of the following match commands. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

- **match [not] message class class_id [id message_id]**—Matches the M3UA message class and type. The following table lists the possible values. Consult M3UA RFCs and documentation for detailed information about these messages.

<table>
<thead>
<tr>
<th>M3UA Message Class</th>
<th>Message ID Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (Management Messages)</td>
<td>0-1</td>
</tr>
<tr>
<td>1 (Transfer Messages)</td>
<td>1</td>
</tr>
<tr>
<td>2 (SS7 Signaling Network Management Messages)</td>
<td>1-6</td>
</tr>
<tr>
<td>3 (ASP State Maintenance Messages)</td>
<td>1-6</td>
</tr>
<tr>
<td>4 (ASP Traffic Maintenance Messages)</td>
<td>1-4</td>
</tr>
<tr>
<td>9 (Routing Key Management Messages)</td>
<td>1-4</td>
</tr>
</tbody>
</table>

- **match [not] opc code**—Matches the originating point code in the data message, that is, the traffic source. Point code is in zone-region-sp format, where the possible values for each element depend on the SS7 variant:
  - **ITU**—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7].
  - **ANSI**—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].
  - **Japan**—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127].
  - **China**—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

- **match [not] dpc code**—Matches the destination point code in the data message. Point code is in zone-region-sp format, as explained for match opc.

- **match [not] service-indicator number**—Matches the service indicator number, 0-15. Following are the available service indicators. Consult M3UA RFCs and documentation for detailed information about these service indicators.
  - 0—Signaling Network Management Messages
  - 1—Signaling Network Testing and Maintenance Messages
  - 2—Signaling Network Testing and Maintenance Special Messages
  - 3—SCCP
  - 4—Telephone User Part
  - 5—ISDN User Part
  - 6—Data User Part (call and circuit-related messages)
  - 7—Data User Part (facility registration and cancellation messages)
Configure an M3UA Inspection Policy Map

- 8—Reserved for MTP Testing User Part
- 9—Broadband ISDN User Part
- 10—Satellite ISDN User Part
- 11—Reserved
- 12—AAL type 2 Signaling
- 13—Bearer Independent Call Control
- 14—Gateway Control Protocol
- 15—Reserved

b) Specify the action you want to perform on the matching traffic by entering one of the following commands:
   - **drop** [log]—Drop all packets that match. Optionally, send a system log message.
   - **rate-limit** *message_rate*—Limit the rate of messages. This option is available with **match message class** only.

   You can specify multiple **match** commands in the policy map. For information about the order of match commands, see How Multiple Traffic Classes are Handled, on page 308.

### Step 4
To configure parameters that affect the inspection engine, perform the following steps:

a) Enter parameters configuration mode:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option:

   - **message-tag-validation** {dupu | error | notify}—Ensures that the content of certain fields are checked and validated for the specified message type. Messages that fail validation are dropped. Validation differs by message type.
     - Destination User Part Unavailable (DUPU)—The User/Cause field must be present, and it must contain only valid cause and user codes.
     - Error—All mandatory fields must be present and contain only allowed values. Each error message must contain the required fields for that error code.
     - Notify—The status type and status information fields must contain allowed values only.

   - **ss7 variant** {ITU | ANSI | JAPAN | CHINA}—Identifies the variant of SS7 used in your network. This option determines the valid format for point codes. After you configure the option and deploy an M3UA policy, you cannot change it unless you first remove the policy. The default variant is ITU.

   - **strict-asp-state**—Performs application server process (ASP) state validation. The system maintains the ASP states of M3UA sessions and allows or drops ASP messages based on the validation result. If you do not enable strict ASP state validation, all ASP messages are forwarded uninspected. Strict ASP state checking is required if you want stateful failover or if you want to operate within a cluster. However, strict ASP state checking works in Override mode only, it does not work if you are running...
in Loadsharing or Broadcast mode (per RFC 4666). The inspection assumes there is one and only one ASP per endpoint.

- **timeout endpoint time**—Sets the idle timeout to remove statistics for an M3UA endpoint, in hh:mm:ss format. To have no timeout, specify 0. The default is 30 minutes (00:30:00).

- **timeout session time**—Sets the idle timeout to remove an M3UA session if you enable strict ASP state validation, in hh:mm:ss format. To have no timeout, specify 0. The default is 30 minutes (00:30:00). Disabling this timeout can prevent the system from removing stale sessions.

### Example

The following is an example of an M3UA policy map and service policy.

```plaintext
hostname(config)# policy-map type inspect m3ua m3ua-map
hostname(config-pmap)# match message class 2 id 6
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match message class 9
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match dpc 1-5-1
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# ss7 variant ITU
hostname(config-pmap-p)# timeout endpoint 00:45:00

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect m3ua m3ua-map

hostname(config)# service-policy global_policy global

What to do next

You can now configure an inspection policy to use the map. See Configure the Mobile Network Inspection Service Policy, on page 425.

### Configure the Mobile Network Inspection Service Policy

Inspections for the protocols used in mobile networks are not enabled in the default inspection policy, so you must enable them if you need these inspections. You can simply edit the default global inspection policy to add these inspections. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

#### Procedure

**Step 1** If necessary, create an L3/L4 class map to identify the traffic for which you want to apply the inspection.

```plaintext
class-map name
```
Configure the Mobile Network Inspection Service Policy

match parameter

Example:

```
hostname(config)# class-map mobile_class_map
hostname(config-cmap)# match access-list mobile
```

In the default global policy, the inspection_default class map is a special class map that includes default ports for all inspection types (match default-inspection-traffic). If you are using this class map in either the default policy or for a new service policy, you can skip this step.

For information on matching statements, see Create a Layer 3/4 Class Map for Through Traffic, on page 295.

Step 2 Add or edit a policy map that sets the actions to take with the class map traffic: policy-map name

Example:

```
hostname(config)# policy-map global_policy
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name.

Step 3 Identify the L3/L4 class map you are using for the inspection: class name

Example:

```
hostname(config-pmap)# class inspection_default
```

To edit the default policy, or to use the special inspection_default class map in a new policy, specify inspection_default for the name. Otherwise, you are specifying the class you created earlier in this procedure.

Step 4 Enable the inspections.

In the following commands, the inspection policy maps are optional. If you created any of these maps to customize the inspection, specify their names on the appropriate command. For Diameter, you can also specify a TLS proxy to enable inspection of encrypted messages.

- **inspect gtp [map_name]**—To enable GTP inspection.
- **inspect sctp [map_name]**—To enable SCTP inspection.
- **inspect diameter [map_name] [tls-proxy proxy_name]**—To enable Diameter inspection.

**Note** If you specify a TLS proxy for Diameter inspection, and you apply NAT port redirection to Diameter server traffic (for example, redirect server traffic from port 5868 to 3868), configure inspection globally or on the ingress interface only. If you apply the inspection to the egress interface, NATed Diameter traffic bypasses inspection.

- **inspect m3ua [map_name]**—To enable M3UA inspection.

Example:

```
hostname(config-class)# inspect gtp
hostname(config-class)# inspect sctp
hostname(config-class)# inspect diameter
```

CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.10
hostname(config-class)# inspect m3ua

**Note**: If you are editing the default global policy (or any in-use policy) to use a different inspection policy map, you must remove the inspection with the `no inspect` version of the command, and then re-add it with the new inspection policy map name. For example, to change the policy map for GTP:

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

**Step 5**: If you are editing an existing service policy (such as the default global policy called `global_policy`), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Example**:

```
hostname(config)# service-policy global_policy global
```

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

---

## Configure RADIUS Accounting Inspection

RADIUS accounting inspection is not enabled by default. You must configure it if you want RADIUS accounting inspection.

**Procedure**

**Step 1** Configure a RADIUS Accounting Inspection Policy Map, on page 427.

**Step 2** Configure the RADIUS Accounting Inspection Service Policy, on page 429.

---

## Configure a RADIUS Accounting Inspection Policy Map

You must create a RADIUS accounting inspection policy map to configure the attributes needed for the inspection.

**Procedure**

**Step 1** Create a RADIUS accounting inspection policy map: `policy-map type inspect radius-accounting policy_map_name`

Where the `policy_map_name` is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2** (Optional) Add a description to the policy map: `description string`
Configure a RADIUS Accounting Inspection Policy Map

**Step 3** Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

**Step 4** Set one or more parameters. You can set the following options; use the `no` form of the command to disable the option.

- **send response**—Instructs the ASA to send Accounting-Request Start and Stop messages to the sender of those messages (which are identified in the `host` command).

- **enable gprs**—Implement GPRS over-billing protection. The ASA checks for the 3GPP VSA 26-10415 attribute in the Accounting-Request Stop and Disconnect messages in order to properly handle secondary PDP contexts. If this attribute is present, then the ASA tears down all connections that have a source IP matching the User IP address on the configured interface.

- **validate-attribute number**—Additional criteria to use when building a table of user accounts when receiving Accounting-Request Start messages. These attributes help when the ASA decides whether to tear down connections.

  If you do not specify additional attributes to validate, the decision is based solely on the IP address in the Framed IP Address attribute. If you configure additional attributes, and the ASA receives a start accounting message that includes an address that is currently being tracked, but the other attributes to validate are different, then all connections started using the old attributes are torn down, on the assumption that the IP address has been reassigned to a new user.

  Values range from 1-191, and you can enter the command multiple times. For a list of attribute numbers and their descriptions, see http://www.iana.org/assignments/radius-types.

- **host ip_address [key secret]**—The IP address of the RADIUS server or GGSN. You can optionally include a secret key so that the ASA can validate the message. Without the key, only the IP address is checked. You can repeat this command to identify multiple RADIUS and GGSNs hosts. The ASA receives a copy of the RADIUS accounting messages from these hosts.

- **timeout users time**—Sets the idle timeout for users (in hh:mm:ss format). To have no timeout, specify 00:00:00. The default is one hour.

**Example**

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345

class-map type management radius-class
  match port udp eq radius-acct

class-map global_policy
  match port udp eq radius-acct
  policy-map global_policy

class radius-class
  inspect radius-accounting radius-acct-pmap
```
Configure the RADIUS Accounting Inspection Service Policy

RADIUS accounting inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. Because RADIUS accounting inspection is for traffic directed to the ASA, you must configure it as a management inspection rule rather than a standard rule.

Procedure

Step 1
Create an L3/L4 management class map to identify the traffic for which you want to apply the inspection, and identify the matching traffic.

```
class-map type management name
match {port | access-list} parameter
```

Example:

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

In this example, the match is for the radius-acct UDP port, which is 1646. You can specify a different port, a range of ports (match port udp range number1 number2) or use match access-list acl_name and use an ACL.

Step 2
Add or edit a policy map that sets the actions to take with the class map traffic: policy-map name

Example:

```
hostname(config)# policy-map global_policy
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name.

Step 3
Identify the L3/L4 management class map you are using for RADIUS accounting inspection: class name

Example:

```
hostname(config-pmap)# class radius-class-map
```

Step 4
Configure RADIUS accounting inspection: inspect radius-accounting [radius-accounting_policy_map]

Where radius_accounting_policy_map is the RADIUS accounting inspection policy map you created in Configure a RADIUS Accounting Inspection Policy Map, on page 427.

Example:

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

Note
If you are editing an in-use policy to use a different inspection policy map, you must remove the RADIUS accounting inspection with the no inspect radius-accounting command, and then re-add it with the new inspection policy map name.
Step 5

If you are editing an existing service policy (such as the default global policy called `global_policy`), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

Example:

```
hostname(config)# service-policy global_policy global
```

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

---

**Monitoring Mobile Network Inspection**

The following topics explain how to monitor mobile network inspection.

**Monitoring GTP Inspection**

To display the GTP configuration, enter the `show service-policy inspect gtp` command in privileged EXEC mode.

Use the `show service-policy inspect gtp statistics` command to show the statistics for GTP inspection. The following is sample output:

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support 0 msg_too_short 0
  unknown_msg 0 unexpected_sig_msg 0
  unexpected_data_msg 0 ie_duplicated 0
  mandatory_ie_missing 0 mandatory_ie_incorrect 0
  optional_ie_incorrect 0 ie_unknown 0
  ie_out_of_order 0 ie_unexpected 0
  total_forwarded 67 total_dropped 1
  signalling_msg_dropped 1 data_msg_dropped 0
  signalling_msg_forwarded 67 data_msg_forwarded 0
  total_created_pdp 33 total_deleted_pdp 32
  total_created_pdpmcb 31 total_deleted_pdpmcb 30
  total_dup_sgw_mcbinfo 0 total_dup_data_mcbinfo 0
  no_new_sgw_sgw_mcbinfo 0 no_new_sgw_data_mcbinfo 0
  pdp_non_existent 1
```

You can get statistics for a specific GTP endpoint by entering the IP address on the `show service-policy inspect gtp statistics ip_address` command.

```
foundation(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
Tunnels Active 0
Tunnels Created 1
Tunnels Destroyed 0
Total Messages Received 1

<table>
<thead>
<tr>
<th>Signalling Messages</th>
<th>Data Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use the `show service-policy inspect gtp pdp-context` command to display PDP context-related information. For GTPv2, this is the bearer context. For example:

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1, TID 050542012151705f, MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22, Idle 0:52:01, Timeout 3:00:00, APN ssenoauth146

Version v2, TID 0505420121517056, MS Addr 100.100.100.102,
SGW Addr 10.0.203.24, Idle 0:00:05, Timeout 3:00:00, APN ssenoauth146

Version v2, TID 0505420121517057, MS Addr 100.100.100.103,
SGW Addr 10.0.203.25, Idle 0:00:04, Timeout 3:00:00, APN ssenoauth146

Version v2, TID 0505420121517055, MS Addr 100.100.100.101,
SGW Addr 10.0.203.23, Idle 0:00:06, Timeout 3:00:00, APN ssenoauth146
```

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

```
Version v1, TID 050542012151705f, MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22, Idle 0:06:14, Timeout 3:00:00, APN ssenoauth146

user_name (IMSI): 505024101215075
nsapi: 5
primary pdp: Y
sgsn is Remote
sgsn addr_signal: 10.0.203.22
sgsn addr_data: 10.0.203.22
ggsn addr_signal: 10.0.202.22
ggsn addr_data: 10.0.202.22
sgsn control teid: 0x00000001
sgsn data teid: 0x000003e8
sgsn control teid: 0x000f4240
sgsn data teid: 0x001e8480
signal_sequence: 18
state: Ready
```

The PDP or bearer context is identified by the tunnel ID (TID), which is a combination of the values for IMSI and NSAPI (GTPv0-1) or IMSI and EBI (GTPv2). A GTP tunnel is defined by two associated contexts in different GSN or SGW/PGW nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile subscriber (MS) user.

### Monitoring SCTP

You can use the following commands to monitor SCTP.

- `show service-policy inspect sctp`
  Displays SCTP inspection statistics. The sctp-drop-override counter increments each time a PPID is matched to a drop action, but the packet was not dropped because it contained data chunks with different PPIDs. For example:

```
ciscoasa# show service-policy inspect sctp
Global policy:
    Service-policy: global_policy
    Class-map: inspection_default
    Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
```
• show scvp [detail]

Displays current SCTP cookies and associations. Add the detail keyword to see detailed information about SCTP associations. The detailed view also shows information about multi-homing, multiple streams, and fragment reassembly.

ciscoasa# show scvp

AssocID: 71adeb15
Local: 192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:

• show conn protocol scvp

Displays information about current SCTP connections.

• show local-host [connection scvp start[-end]]

Displays information on hosts making SCTP connections through the ASA, per interface. Add the connection scvp keyword to see only those hosts with the specified number or range of SCTP connections.

• show traffic

Displays SCTP connection and inspection statistics per interface if you enable the sysopt traffic detailed-statistics command.

Monitoring Diameter

You can use the following commands to monitor Diameter.

• show service-policy inspect diameter

Displays Diameter inspection statistics. For example:

ciscoasa# show service-policy inspect diameter

Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
  Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
  5-min-pkt-rate 0 pkts/sec, v6-fall-close 0
  Class-map: log_app
  Log: 5849
Class-map: block_ip
drop-connection: 2

• **show diameter**
  
  Displays state information for each Diameter connection. For example:

  ```
  ciscoasa# show diameter
  Total active diameter sessions: 5
  Session 3638
  =========
  ref_count: 1 val = .; 10962988391; 2461;
  Protocol : diameter Context id : 0
  From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
  ...
  ```

• **show conn detail**
  
  Displays connection information. Diameter connections are marked with the Q flag.

• **show tls-proxy**
  
  Displays information about the TLS proxy if you use one in Diameter inspection.

---

**Monitoring M3UA**

You can use the following commands to monitor M3UA.

• **show service-policy inspect m3ua drops**
  
  Displays drop statistics for M3UA inspection.

• **show service-policy inspect m3ua endpoint [IP_address]**
  
  Displays statistics for M3UA endpoints. You can specify an endpoint IP address to see information for a specific endpoint. For high availability or clustered systems, the statistics are per unit, they are not synchronized across units. For example:

  ```
  ciscoasa# sh service-policy inspect m3ua endpoint
  M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
   All Messages 21 5 26
   DATA Messages 9 5 14
  M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
   All Messages 21 8 29
   DATA Messages 9 8 17
  ```

• **show service-policy inspect m3ua session**
  
  Displays information about M3UA sessions if you enable strict application server process (ASP) state validation. Information includes source association ID, whether the session is single or double exchange, and in clustering, whether it is a cluster owner session or a backup session. In a cluster with 3 or more units, you might see stale backup sessions if a unit leaves and then returns to the cluster. These stale sessions are removed when they time out, unless you disabled session timeout.
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
d - double exchange , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os

- show service-policy inspect m3ua table
Displays the run-time M3UA inspection table, including classification rules.

- show conn detail
Displays connection information. M3UA connections are marked with the v flag.

### History for Mobile Network Inspection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPv2 inspection and improvements to GTPv0/1 inspection.</td>
<td>9.5(1)</td>
<td>GTP inspection can now handle GTPv2. In addition, GTP inspection for all versions now supports IPv6 addresses. We changed the <code>match message id</code> command to `match message {v1</td>
</tr>
<tr>
<td>SCTP inspection</td>
<td>9.5(2)</td>
<td>You can now apply application-layer inspection to Stream Control Transmission Protocol (SCTP) traffic to apply actions based on payload protocol identifier (PPID). We added or modified the following commands: <code>clear conn protocol scctp, inspect scctp, match ppid, policy-map type inspect scctp, show conn protocol scctp, show local-host connection scctp, show service-policy inspect scctp.</code></td>
</tr>
<tr>
<td>Diameter inspection</td>
<td>9.5(2)</td>
<td>You can now apply application-layer inspection to Diameter traffic and also apply actions based on application ID, command code, and attribute-value pair (AVP) filtering. We added or modified the following commands: <code>class-map type inspect diameter, diameter, inspect diameter, match application-id, match avp, match command-code, policy-map type inspect diameter, show conn detail, show diameter, show service-policy inspect diameter, unsupported.</code></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Diameter inspection improvements</td>
<td>9.6(1)</td>
<td>You can now inspect Diameter over TCP/TLS traffic, apply strict protocol conformance checking, and inspect Diameter over SCTP in cluster mode. We added or modified the following commands: <code>client clear-text</code>, <code>inspect diameter</code>, <code>strict-diameter</code>.</td>
</tr>
<tr>
<td>SCTP stateful inspection in cluster mode</td>
<td>9.6(1)</td>
<td>SCTP stateful inspection now works in cluster mode. You can also configure SCTP stateful inspection bypass in cluster mode. We did not introduce or change any commands.</td>
</tr>
<tr>
<td>MTP3 User Adaptation (M3UA) inspection.</td>
<td>9.6(2)</td>
<td>You can now inspect M3UA traffic and also apply actions based on point code, service indicator, and message class and type. We added or modified the following commands: `clear service-policy inspect m3ua {drops</td>
</tr>
<tr>
<td>Support for SCTP multi-streaming reordering and reassembly and fragmentation. Support for SCTP multi-homing, where the SCTP endpoints have more than one IP address.</td>
<td>9.7(1)</td>
<td>The system now fully supports SCTP multi-streaming reordering, reassembly, and fragmentation, which improves Diameter and M3UA inspection effectiveness for SCTP traffic. The system also supports SCTP multi-homing, where the endpoints have more than one IP address each. For multi-homing, the system opens pinholes for the secondary addresses so that you do not need to write access rules to allow them. SCTP endpoints must be limited to 3 IP addresses each. We modified the output of the following command: <code>show sctp detail</code>.</td>
</tr>
<tr>
<td>M3UA inspection improvements.</td>
<td>9.7(1)</td>
<td>M3UA inspection now supports stateful failover, semi-distributed clustering, and multihoming. You can also configure strict application server process (ASP) state validation and validation for various messages. Strict ASP state validation is required for stateful failover and clustering. We added or modified the following commands: <code>clear service-policy inspect m3ua session [assocID id]</code>, <code>match port sctp</code>, <code>message-tag-validation</code>, <code>show service-policy inspect m3ua drop</code>, <code>show service-policy inspect m3ua endpoint</code>, <code>show service-policy inspect m3ua session</code>, <code>show service-policy inspect m3ua table</code>, <code>strict-asp-state</code>, <code>timeout session</code>.</td>
</tr>
<tr>
<td>Support for setting the TLS proxy server SSL cipher suite.</td>
<td>9.8(1)</td>
<td>You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the <code>ssl cipher</code> command. We introduced the following command: <code>server cipher-suite</code></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GTP inspection enhancements for MSISDN and Selection Mode filtering, anti-replay, and user spoofing protection.</td>
<td>9.10(1)</td>
<td>You can now configure GTP inspection to drop Create PDP Context messages based on Mobile Station International Subscriber Directory Number (MSISDN) or Selection Mode. You can also implement anti-replay and user spoofing protection. We added the following commands: <code>anti-replay</code>, <code>gtp-u-header-check</code>, <code>match msisdn</code>, <code>match selection-mode</code>.</td>
</tr>
</tbody>
</table>
PART V

Connection Management and Threat Detection

• Connection Settings, on page 439
• Quality of Service, on page 465
• Threat Detection, on page 479
Connection Settings

This chapter describes how to configure connection settings for connections that go through the ASA, or for management connections that go to the ASA.

• What Are Connection Settings?, on page 439
• Configure Connection Settings, on page 440
• Monitoring Connections, on page 461
• History for Connection Settings, on page 462

What Are Connection Settings?

Connection settings comprise a variety of features related to managing traffic connections, such as a TCP flow through the ASA. Some features are named components that you would configure to supply specific services.

Connection settings include the following:

• **Global timeouts for various protocols**—All global timeouts have default values, so you need to change them only if you are experiencing premature connection loss.

• **Connection timeouts per traffic class**—You can override the global timeouts for specific types of traffic using service policies. All traffic class timeouts have default values, so you do not have to set them.

• **Connection limits and TCP Intercept**—By default, there are no limits on how many connections can go through (or to) the ASA. You can set limits on particular traffic classes using service policy rules to protect servers from denial of service (DoS) attacks. Particularly, you can set limits on embryonic connections (those that have not finished the TCP handshake), which protects against SYN flooding attacks. When embryonic limits are exceeded, the TCP Intercept component gets involved to proxy connections and ensure that attacks are throttled.

• **Dead Connection Detection (DCD)**—If you have persistent connections that are valid but often idle, so that they get closed because they exceed idle timeout settings, you can enable Dead Connection Detection to identify idle but valid connections and keep them alive (by resetting their idle timers). Whenever idle times are exceeded, DCD probes both sides of the connection to see if both sides agree the connection is valid. The `show service-policy` command output includes counters to show the amount of activity from DCD.

• **TCP sequence randomization**—Each TCP connection has two initial sequence numbers (ISN): one generated by the client and one generated by the server. By default, the ASA randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions. Randomization prevents an attacker
from predicting the next ISN for a new connection and potentially hijacking the new session. You can disable randomization per traffic class if desired.

- **TCP Normalization**—The TCP Normalizer protects against abnormal packets. You can configure how some types of packet abnormalities are handled by traffic class.

- **TCP State Bypass**—You can bypass TCP state checking if you use asymmetrical routing in your network.

- **SCTP State Bypass**—You can bypass Stream Control Transmission Protocol (SCTP) stateful inspection if you do not want SCTP protocol validation.

- **Flow offloading**—You can identify select traffic to be offloaded to a super fast path, where the flows are switched in the NIC itself. Offloading can help you improve performance for data-intensive applications such as large file transfers.

**Configure Connection Settings**

Connection limits, timeouts, TCP Normalization, TCP sequence randomization, and decrementing time-to-live (TTL) have default values that are appropriate for most networks. You need to configure these connection settings only if you have unusual requirements, your network has specific types of configuration, or if you are experiencing unusual connection loss due to premature idle timeouts.

Other connection-related features are not enabled. You would configure these services on specific traffic classes only, and not as a general service. These features include the following: TCP Intercept, TCP State Bypass, Dead Connection Detection (DCD), SCTP state bypass, flow offload.

The following general procedure covers the gamut of possible connection setting configurations. Pick and choose which to implement based on your needs.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Configure Global Timeouts</strong>, on page 441. These settings change the default idle timeouts for various protocols for all traffic that passes through the device. If you are having problems with connections being reset due to premature timeouts, first try changing the global timeouts.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>Protect Servers from a SYN Flood DoS Attack (TCP Intercept)</strong>, on page 443. Use this procedure to configure TCP Intercept.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer)</strong>, on page 445, if you want to alter the default TCP Normalization behavior for specific traffic classes.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass)</strong>, on page 449, if you have this type of routing environment.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>Disable TCP Sequence Randomization</strong>, on page 452, if the default randomization is scrambling data for certain connections.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>Offload Large Flows</strong>, on page 454, if you need to improve performance in a computing intensive data center.</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>Configure Connection Settings for Specific Traffic Classes (All Services)</strong>, on page 457. This is a catch-all procedure for connection settings. These settings can override the global defaults for specific traffic classes using service policy rules. You also use these rules to customize TCP Normalizer, change TCP sequence randomization, decrement time-to-live on packets, and implement other optional features.</td>
</tr>
</tbody>
</table>
Configure Global Timeouts

You can set the global idle timeout durations for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool.

Changing the global timeout sets a new default timeout, which in some cases can be overridden for particular traffic flows through service policies.

Procedure

Use the `timeout` command to set global timeouts.

All timeout values are in the format `hh:mm:ss`, with a maximum duration of 1193:0:0 in most cases. Use the `no timeout` command to reset all timeouts to their default values. If you want to simply reset one timer to the default, enter the `timeout` command for that setting with the default value.

Use `0` for the value to disable a timer.

You can configure the following global timeouts.

- **timeout conn hh:mm:ss** — The idle time after which a connection closes, between 0:5:0 and 1193:0:0. The default is 1 hour (1:0:0).

- **timeout half-closed hh:mm:ss** — The idle time until a TCP half-closed connection closes. The minimum is 30 seconds. The default is 10 minutes.

- **timeout udp hh:mm:ss** — The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.

- **timeout icmp hh:mm:ss** — The idle time for ICMP, between 0:0:2 and 1193:0:0. The default is 2 seconds (0:0:2).

- **timeout icmp-error hh:mm:ss** — The idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet, between 0:0:0 and 0:1:0 or the `timeout icmp` value, whichever is lower. The default is 0 (disabled). When this timeout is disabled, and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors.

- **timeout sunrpc hh:mm:ss** — The idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.

- **timeout H323 hh:mm:ss** — The idle time after which H.245 (TCP) and H.323 (UDP) media connections close, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.

- **timeout h225 hh:mm:ss** — The idle time until an H.225 signaling connection closes. The H.225 default timeout is 1 hour (1:0:0). To close a connection immediately after all calls are cleared, a value of 1 second (0:0:1) is recommended.

- **timeout mgcp hh:mm:ss** — The idle time after which an MGCP media connection is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0)

- **timeout mgcp-pat hh:mm:ss** — The absolute interval after which an MGCP PAT translation is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The minimum time is 30 seconds.
• **timeout sctp hh:mm:ss**—The idle time until a Stream Control Transmission Protocol (SCTP) connection closes, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).

• **timeout sip hh:mm:ss**—The idle time until a SIP signaling port connection closes, between 0:5:0 and 1193:0:0. The default is 30 minutes (0:30:0).

• **timeout sip_media hh:mm:ss**—The idle time until an SIP media port connection closes. This duration must be at least 1 minute. The default is 2 minutes. The SIP media timer is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.

• **timeout sip-provisional-media hh:mm:ss**—The timeout value for SIP provisional media connections, between 0:1:0 and 0:30:0. The default is 2 minutes.

• **timeout sip-invite hh:mm:ss**—The idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 00:30:0. The default is 3 minutes (0:3:0).

• **timeout sip-disconnect hh:mm:ss**—The idle time after which a SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 00:10:0. The default is 2 minutes (0:2:0).

• **timeout uauth hh:mm:ss {absolute | inactivity}**—The duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The default timer is **absolute**; you can set the timeout to occur after a period of inactivity by entering the **inactivity** keyword. The uauth duration must be shorter than the xlate duration. Set to 0 to disable caching. Do not use 0 if passive FTP is used for the connection or if the virtual http command is used for web authentication.

• **timeout xlate hh:mm:ss**—The idle time until a translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.

• **timeout pat-xlate hh:mm:ss**—The idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.

• **timeout tcp-proxy-reassembly hh:mm:ss**—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).

• **timeout floating-conn hh:mm:ss**—When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0.

• **timeout conn-holddown hh:mm:ss**—How long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. The purpose of the connection holddown timer is to reduce the effect of route flapping, where routes might come up and go down quickly. You can reduce the holddown timer to make route convergence happen more quickly. The default is 15 seconds, the range is 00:00:00 to 00:00:15.
• **timeout igp stale-route hh:mm:ss**—How long to keep a stale route before removing it from the router information base. These routes are for interior gateway protocols such as OSPF. The default is 70 seconds (00:01:10), the range is 00:00:10 to 00:01:40.

---

**Protect Servers from a SYN Flood DoS Attack (TCP Intercept)**

A SYN-flooding denial of service (DoS) attack occurs when an attacker sends a series of SYN packets to a host. These packets usually originate from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests from legitimate users.

You can limit the number of embryonic connections to help prevent SYN flooding attacks. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request using the SYN cookie method (see Wikipedia for details on SYN cookies). When the ASA receives an ACK back from the client, it can then authenticate that the client is real and allow the connection to the server. The component that performs the proxy is called TCP Intercept.

The end-to-end process for protecting a server from a SYN flood attack involves setting connection limits, enabling TCP Intercept statistics, and then monitoring the results.

**Before you begin**

- Ensure that you set the embryonic connection limit lower than the TCP SYN backlog queue on the server that you want to protect. Otherwise, valid clients can no longer access the server during a SYN attack. To determine reasonable values for embryonic limits, carefully analyze the capacity of the server, the network, and server usage.

- Depending on the number of CPU cores on your ASA model, the maximum concurrent and embryonic connections can exceed the configured numbers due to the way each core manages connections. In the worst case scenario, the ASA allows up to \( n-1 \) extra connections and embryonic connections, where \( n \) is the number of cores. For example, if your model has 4 cores, if you configure 6 concurrent connections and 4 embryonic connections, you could have an additional 3 of each type. To determine the number of cores for your model, enter the `show cpu core` command.

**Procedure**

**Step 1** Create an L3/L4 class map to identify the servers you are protecting. Use an access-list match.

```plaintext
class-map name
match parameter
```

**Example:**

```plaintext
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```
**Step 2** Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

```
policy-map name
class name
```

**Example:**

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

In the default configuration, the `global_policy` policy map is assigned globally to all interfaces. If you want to edit the `global_policy`, enter `global_policy` as the policy name. For the class map, specify the class you created earlier in this procedure.

**Step 3** Set the embryonic connection limits.

- **set connection embryonic-conn-max n**—The maximum number of simultaneous embryonic TCP connections allowed, between 0 and 2000000. The default is 0, which allows unlimited connections.

- **set connection per-client-embryonic-max n**—The maximum number of simultaneous embryonic TCP connections allowed per client, between 0 and 2000000. The default is 0, which allows unlimited connections.

**Example:**

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

**Step 4** If you are editing an existing service policy (such as the default global policy called `global_policy`), you can skip this step. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Example:**

```
hostname(config)# service-policy global_policy global
```

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

**Step 5** Configure threat detection statistics for attacks intercepted by TCP Intercept.

```
threat-detection statistics tcp-intercept [rate-interval minutes] [burst-rate attacks_per_sec] [average-rate attacks_per_sec]
```

Where:

- **rate-interval minutes** sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the ASA samples the number of attacks 30 times.

- **burst-rate attacks_per_sec** sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
- **average-rate** attacks per sec sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.

**Example:**

```bash
hostname(config)# threat-detection statistics tcp-intercept
```

**Step 6** Monitor the results with the following commands:

- **show threat-detection statistics top tcp-intercept [all | detail]** — View the top 10 protected servers under attack. The `all` keyword shows the history data of all the traced servers. The `detail` keyword shows history sampling data. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.

- **clear threat-detection statistics tcp-intercept** — Erases TCP Intercept statistics.

**Example:**

```bash
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins  Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
----------------------------------------------------------------------------------
1 10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2 10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

---

**Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer)**

The TCP Normalizer identifies abnormal packets that the ASA can act on when they are detected; for example, the ASA can allow, drop, or clear the packets. TCP normalization helps protect the ASA from attacks. TCP normalization is always enabled, but you can customize how some features behave.

The default configuration includes the following settings:

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
```
To customize the TCP normalizer, first define the settings using a TCP map. Then, you can apply the map to selected traffic classes using service policies.

**Procedure**

**Step 1**
Create a TCP map to specify the TCP normalization criteria that you want to look for: `tcp-map tcp-map-name`

**Step 2**
Configure the TCP map criteria by entering one or more of the following commands. The defaults are used for any commands you do not enter. Use the `no` form of a command to disable the setting.

- **check-retransmission**—Prevent inconsistent TCP retransmission. This command is disabled by default.

- **checksum-verification**—Verify the TCP checksum, dropping packets that fail verification. This command is disabled by default.

- **exceed-mss** `{allow | drop}`—Allow or drop packets whose data length exceeds the TCP maximum segment size. The default is to allow the packets.

- **invalid-ack** `{allow | drop}`—Allow or drop packets with an invalid ACK. The default is to drop the packet, with the exception of WAAS connections, where they are allowed. 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 the 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.

- **queue-limit** `pkt_num [timeout seconds]`—Set the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, between 1 and 250 packets. 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 (the `inspect` command), IPS (the `ips` command), and TCP check-retransmission (the TCP map `check-retransmission` command) have a queue limit of 3 packets. If the ASA 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 example, for application inspection, IPS, and TCP check-retransmission traffic, any advertised settings from TCP packets are ignored in favor of the `queue-limit` setting. For other TCP traffic, out-of-order packets are now buffered and put in order instead of passed through untouched.

The `timeout seconds` argument sets 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 `pkt_num` argument is set to 0; you need to set the limit to be 1 or above for the `timeout` keyword to take effect.
- **reserved-bits** {allow | clear | drop}—Set the action for reserved bits in the TCP header. You can allow the packet (without changing the bits), clear the bits and allow the packet, or drop the packet.

- **seq-past-window** {allow | drop}—Set the action for 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. You can allow the packets only if the queue-limit command is set to 0 (disabled). The default is to drop the packets.

- **synack-data** {allow | drop}—Allow or drop TCP SYNACK packets that contain data. The default is to drop the packet.

- **syn-data** {allow | drop}—Allow or drop SYN packets with data. The default is to allow the packet.

- **tcp-options** {md5 | mss | selective-ack | timestamp | window-scale | range lower upper} action—Set the action for packets with TCP options. These options are named: md5, mss, selective-ack (selective acknowledgment mechanism), timestamp, and window-scale (window scale mechanism). For other options, you specify them by number on the range keyword, where the range limits are 6-7, 9-18, and 20-255. To target a single option by number, enter the same number for the lower and upper range. You can enter the command multiple times in a map to define your complete policy. Note that if a TCP connection is inspected, all options are cleared except the MSS and selective-acknowledgment (SACK) options, regardless of your configuration. Following are the possible actions:
  - **allow [multiple]**—Allow packets that contain a single option of this type. This is the default for all of the named options. If you want to allow packets even if they contain more than one instance of the option, add the multiple keyword. (The multiple keyword is not available with range.)

  - **maximum limit**—For mss only. Set the maximum segment size to the indicated limit, from 68-65535. The default TCP MSS is defined on the sysopt connection tcpmss command.

  - **clear**—Remove the options of this type from the header and allow the packet. This is the default for all of the numbered options. Note that clearing the timestamp option disables PAWS and RTT.

  - **drop**—Drop packets that contain this option. This action is available for md5 and range only.

- **ttl-evasion-protection**—Have the maximum TTL for a connection be determined by the TTL in the initial packet. The TTL for subsequent packets can decrease, but it cannot increase. The system will reset the TTL to the lowest previously-seen TTL for that connection. This protects against TTL evasion attacks. TTL evasion protection is enabled by default, so you would only need to enter the **no** form of this command.

  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 ASA 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 ASA 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.

- **urgent-flag** {allow | clear}—Set the action for packets with the URG flag. You can allow the packet, or clear the flag and allow the packet. The default is to clear the flag.

  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.

- **window-variation** {allow | drop}—Allow or drop a connection that has changed its window size unexpectedly. The default is to allow the connection.
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.

**Step 3**  
Apply the TCP map to a traffic class using a service policy.

a) Define the traffic class with an L3/L4 class map and add the map to a policy map.

```
class-map name
match parameter
policy-map name
class name
```

**Example:**

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. For information on matching statements for class maps, see Create a Layer 3/4 Class Map for Through Traffic, on page 295.

b) Apply the TCP map: `set connection advanced-options tcp-map-name`

**Example:**

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

c) If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Example:**

```
hostname(config)# service-policy global_policy global
```

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

---

**Examples**

For example, to allow urgent flag and urgent offset packets for all traffic sent to the range of TCP ports between the well known FTP data port and the Telnet port, enter the following commands:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
```
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global

Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass)

If you have an asynchronous routing environment in your network, where the outbound and inbound flow for a given connection can go through two different ASA devices, you need to implement TCP State Bypass on the affected traffic.

However, TCP State Bypass weakens the security of your network, so you should apply bypass on very specific, limited traffic classes.

The following topics explain the problem and solution in more detail.

The Asynchronous Routing Problem

By default, all traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. The ASA maximizes the firewall performance by checking the state of each packet (new connection or established connection) and assigning it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection).

TCP packets that match existing connections in the fast path can pass through the ASA without rechecking every aspect of the security policy. This feature maximizes performance. However, the method of establishing the session in the fast path using the SYN packet, and the checks that occur in the fast path (such as TCP sequence number), can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow of a connection must pass through the same ASA.

For example, a new connection goes to Security Appliance 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through Security Appliance 1, then the packets match the entry in the fast path, and are passed through. But if subsequent packets go to Security Appliance 2, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped. The following figure shows an asymmetric routing example where the outbound traffic goes through a different ASA than the inbound traffic:
If you have asymmetric routing configured on upstream routers, and traffic alternates between two ASA devices, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet matching the specified networks enters the ASA, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

**Guidelines and Limitations for TCP State Bypass**

**TCP State Bypass Unsupported Features**

The following features are not supported when you use TCP state bypass:

- Application inspection—Inspection requires both inbound and outbound traffic to go through the same ASA, so inspection is not applied to TCP state bypass traffic.
- AAA authenticated sessions—When a user authenticates with one ASA, traffic returning via the other ASA will be denied because the user did not authenticate with that ASA.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The ASA does not keep track of the state of the connection, so these features are not applied.
- TCP normalization—The TCP normalizer is disabled.
- Service module functionality—You cannot use TCP state bypass and any application running on any type of service module, such as ASA FirePOWER.
- Stateful failover.
TCP State Bypass NAT Guidelines

Because the translation session is established separately for each ASA, be sure to configure static NAT on both devices for TCP state bypass traffic. If you use dynamic NAT, the address chosen for the session on Device 1 will differ from the address chosen for the session on Device 2.

Configure TCP State Bypass

To bypass TCP state checking in asynchronous routing environments, carefully define a traffic class that applies to the affected hosts or networks only, then enable TCP State Bypass on the traffic class using a service policy. Because bypass reduces the security of the network, limit its application as much as possible.

Before you begin

If there is no traffic on a given connection for 2 minutes, the connection times out. You can override this default using the `set connection timeout idle` command for the TCP state bypass traffic class. Normal TCP connections timeout by default after 60 minutes.

Procedure

Step 1  Create an L3/L4 class map to identify the hosts that require TCP State Bypass. Use an access-list match to identify the source and destination hosts.

```config
class-map name
match parameter
```

Example:

```config
hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2
hostname(config)# class-map bypass-class
hostname(config-cmap)# match access-list bypass
```

Step 2  Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

```config
policy-map name
class name
```

Example:

```config
hostname(config)# policy-map global_policy
hosname(config-pmap)# class bypass-class
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. For the class map, specify the class you created earlier in this procedure.

Step 3  Enable TCP State Bypass on the class: `set connection advanced-options tcp-state-bypass`

Step 4  If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```
Example:

hostname(config)# service-policy global_policy global

The `global` keyword applies the policy map to all interfaces, and `interface` applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

Example

The following is a sample configuration for TCP state bypass:

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass
hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass
hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

Disable TCP Sequence Randomization

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The ASA 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.

You can disable TCP initial sequence number randomization if necessary, for example, because data is getting scrambled. 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 ASA, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.

- You use a WAAS device that requires the ASA not to randomize the sequence numbers of connections.

- You enable hardware bypass for the ISA 3000, and TCP connections are dropped when the ISA 3000 is no longer part of the data path.
Procedure

Step 1  Create an L3/L4 class map to identify the traffic whose TCP sequence numbers should not be randomized. The class match should be for TCP traffic; you can identify specific hosts (with an ACL), do a TCP port match, or simply match any traffic.

```plaintext
class-map name
match parameter

Example:

hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

Step 2  Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

```plaintext
policy-map name
class name

Example:

hostname(config)# policy-map global_policy
hostname(config-pmap)# class preserve-sq-no
```

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. For the class map, specify the class you created earlier in this procedure.

Step 3  Disable TCP sequence number randomization on the class: set connection random-sequence-number disable
If you later decide to turn it back on, replace “disable” with enable.

Step 4  If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

```plaintext
service-policy policymap_name {global | interface interface_name}

Example:

hostname(config)# service-policy global_policy global
```

The global keyword applies the policy map to all interfaces, and interface applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.
Offload Large Flows

If you deploy the ASA on the Firepower 4100/9300 chassis (FXOS 1.1.3 or later) in a data center, you can identify select traffic to be offloaded to a super fast path, where traffic is switched in the NIC itself. Offloading can help you improve performance for data-intensive applications such as large file transfers.

- High Performance Computing (HPC) Research sites, where the ASA is deployed between storage and high compute stations. When one research site backs up using FTP file transfer or file sync over NFS, the large amount of data traffic affects all contexts on the ASA. Offloading FTP file transfer and file sync over NFS reduces the impact on other traffic.

- High Frequency Trading (HFT), where the ASA is deployed between workstations and the Exchange, mainly for compliance purposes. Security is usually not a concern, but latency is a major concern.

Before being offloaded, the ASA first applies normal security processing, such as access rules and inspection, during connection establishment. The ASA also does session tear-down. But once a connection is established, if it is eligible to be offloaded, further processing happens in the NIC rather than the ASA.

Offloaded flows continue to receive limited stateful inspection, such as basic TCP flag and option checking, and checksum verification if you configure it. The system can selectively escalate packets to the firewall system for further processing if necessary.

To identify flows that can be offloaded, you create a service policy rule that applies the flow offloading service. A matching flow is then offloaded if it meets the following conditions:

- IPv4 addresses only.
- TCP, UDP, GRE only.
- Standard or 802.1Q tagged Ethernet frames only.
- (Transparent mode only.) Multicast flows for bridge groups that contain two and only two interfaces.

Reverse flows for offloaded flows are also offloaded.

Flow Offload Limitations

Not all flows can be offloaded. Even after offload, a flow can be removed from being offloaded under certain conditions. Following are some of the limitations:

Flows that cannot be offloaded

The following types of flows cannot be offloaded.

- Flows that use IPv6 addressing.
- Flows for any protocol other than TCP, UDP, and GRE.

Note

PPTP GRE connections cannot be offloaded.

- Flows that require inspection. In some cases, such as FTP, the secondary data channel can be offloaded although the control channel cannot be offloaded.
- Flows that pass through another module, such as ASA Firepower.
• IPSec and VPN connections.
• Flows for which you decrement the time-to-live (TTL) value.
• Flows that require encryption or decryption.
• Multicast flows in routed mode.
• Multicast flows in transparent mode for bridge groups that have three or more interfaces.
• TCP Intercept flows.
• AAA-related flows.
• Vpath, VXLAN related flows.
• URL filtering.
• Tracer flows.
• Flows tagged with security groups.
• Reverse flows that are forwarded from a different cluster node, in case of asymmetric flows in a cluster.
• Centralized flows in a cluster, if the flow owner is not the master.

Conditions for reversing offload

After a flow is offloaded, packets within the flow are returned to the ASA for further processing if they meet the following conditions:

• They include TCP options other than Timestamp.
• They are fragmented.
• They are subject to Equal-Cost Multi-Path (ECMP) routing, and ingress packets move from one interface to another.

Configure Flow Offload

To configure flow offload, you must enable the service and then create service policies to identify the traffic that is eligible for offloading. Enabling or disabling the service requires a reboot. However, adding or editing service policies does not require a reboot.

Flow offloading is available on the ASA on the Firepower 4100/9300 chassis (FXOS 1.1.3 or later) only.

Note


Procedure

Step 1
Enable the flow offload service.

flow-offload enable
You must reload the system whenever you enable or disable the service.

In multiple-context mode, enabling or disabling flow offload enables or disables it for all contexts. You cannot have different settings per context.

There are special considerations for changing the mode for clusters or failover pairs if you want a hitless change:

- **Clustering**—First enter the command on the master unit, but do not reboot the master unit immediately. Instead, reboot each member of the cluster first, then return to the master and reboot it. You can then configure the offloading service policy on the master unit.
- **Failover**—First enter the command on the active unit, but do not reboot it immediately. Instead, reboot the standby unit, then reboot the active unit. You can then configure the offloading service policy on the active unit.

**Example:**

ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is saved and the system has been rebooted.

ciscoasa(config)# write memory

ciscoasa(config)# reload

**Step 2**

Create the service policy rule that identifies traffic that is eligible for offload.

a) Create an L3/L4 class map to identify the traffic that is eligible for flow offload. Matching by access-list or port would be the most typical options.

    class-map name
    match parameter

**Example:**

hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload

b) Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

    policy-map name
    class name

**Example:**

hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload

In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. For the class map, specify the class you created earlier in this procedure.
c) Enable flow offload on the class: **set connection advanced-options flow-offload**

d) If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

Example:

```
hostname(config)# service-policy offload_policy interface outside
```

The **global** keyword applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

---

**Example**

The following example classifies all TCP traffic from the 10.1.1.0 255.255.255.224 subnet as eligible for offload and attaches the policy to the outside interface.

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

---

**Configure Connection Settings for Specific Traffic Classes (All Services)**

You can configure different connection settings for specific traffic classes using service policies. Use service policies to:

- Customize connection limits and timeouts used to protect against DoS and SYN-flooding attacks.
- Implement Dead Connection Detection so that valid but idle connections remain alive.
- Disable TCP sequence number randomization in cases where you do not need it.
- Customize how the TCP Normalizer protects against abnormal TCP packets.
- Implement TCP State Bypass for traffic subject to asynchronous routing. Bypass traffic is not subject to inspection.
- Implement Stream Control Transmission Protocol (SCTP) State Bypass to turn off SCTP stateful inspection.
- Implement flow offload to improve performance on supported hardware platforms.
- Decrement time-to-live (TTL) on packets so that the ASA will show up on trace route output.
If you decrement time to live, packets with a TTL of 1 will be dropped, but a connection will be opened for the session on the assumption that the connection might contain packets with a greater TTL. Note that some packets, such as OSPF hello packets, are sent with TTL = 1, so decrementing time to live can have unexpected consequences.

You can configure any combination of these settings for a given traffic class, except for TCP State Bypass and TCP Normalizer customization, which are mutually exclusive.

This procedure shows a service policy for traffic that goes through the ASA. You can also configure the connection maximum and embryonic connection maximum for management (to the box) traffic.

**Before you begin**

If you want to customize the TCP Normalizer, create the required TCP Map before proceeding.

The `set connection` command (for connection limits and sequence randomization) and `set connection timeout` commands are described here separately for each parameter. However, you can enter the commands on one line, and if you enter them separately, they are shown in the configuration as one command.

**Procedure**

**Step 1**

Create an L3/L4 class map to identify the traffic for which you want to customize connection settings.

```plaintext
class-map name
match parameter
```

**Example:**

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

For information on matching statements, see Create a Layer 3/4 Class Map for Through Traffic, on page 295.

**Step 2**

Add or edit a policy map that sets the actions to take with the class map traffic, and identify the class map.

```plaintext
policy-map name
class name
```

**Example:**

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class CONNS
```
In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. For the class map, specify the class you created earlier in this procedure.

**Step 3**

Set connection limits and TCP sequence number randomization. (TCP Intercept.)

- **set connection conn-max n**—(TCP, UDP, SCTP.) The maximum number of simultaneous connections that are allowed, between 0 and 2000000, for the entire class. The default is 0, which allows unlimited connections. For TCP connections, this applies to established connections only.
  - If two servers are configured to allow simultaneous connections, the connection limit is applied to each configured server separately.
  - Because the limit is applied to a class, one attack host can consume all the connections and leave none for the rest of the hosts that are matched to the class.

- **set connection embryonic-conn-max n**—The maximum number of simultaneous embryonic TCP connections allowed, between 0 and 2000000. The default is 0, which allows unlimited connections. By setting a non-zero limit, you enable TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. Also set the per-client options to protect against SYN flooding.

- **set connection per-client-embryonic-max n**—The maximum number of simultaneous embryonic TCP connections allowed per client, between 0 and 2000000. The default is 0, which allows unlimited connections.

- **set connection per-client-max n**—(TCP, UDP, SCTP.) The maximum number of simultaneous connections allowed per client, between 0 and 2000000. The default is 0, which allows unlimited connections. This argument restricts the maximum number of simultaneous connections that are allowed for each host that is matched to the class. For TCP connections, this includes established, half-open, and half-closed connections.

- **set connection random-sequence-number {enable | disable}**—Whether to enable or disable TCP sequence number randomization. Randomization is enabled by default.

**Example:**

`hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable`

**Step 4**

Set connection timeouts and Dead Connection Detection (DCD).

The defaults described below assume you have not changed the global defaults for these behaviors using the `timeout` command; the global defaults override the ones described here. Enter 0 to disable the timer, so that a connection never times out.

- **set connection timeout embryonic hh:mm:ss**—The timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:00:00. The default is 0:0:30.

- **set connection timeout idle hh:mm:ss [reset]**—The idle timeout period after which an established connection of any protocol closes, between 0:0:1 and 1193:0:0. The default is 1:0:0. For TCP traffic, the `reset` keyword sends a reset to TCP endpoints when the connection times out.

  The default `udp` idle timeout is 2 minutes. The default `icmp` idle timeout is 2 seconds. The default `esp` and `ha` idle timeout is 30 seconds. For all other protocols, the default idle timeout is 2 minutes.
• **set connection timeout half-closed hh:mm:ss**—The idle timeout period until a half-closed connection is closed, between 0:5:0 (for 9.1(1) and earlier) or 0:30:0 (for 9.1(2) and later) and 1193:0:0. The default is 0:10:0. Half-closed connections are not affected by DCD. Also, the ASA does not send a reset when taking down half-closed connections.

• **set connection timeout dcd [retry-interval [max_retries]]**—Enable Dead Connection Detection (DCD). Before expiring an idle connection, the ASA probes the end hosts to determine if the connection is valid. If both hosts respond, the connection is preserved, otherwise the connection is freed. When operating in transparent firewall mode, you must configure static routes for the endpoints. You cannot use DCD in a cluster.

  The retry-interval sets the time duration in *hh:mm:ss* format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15. The max-retries sets the number of consecutive failed retries for DCD before declaring the connection as dead. The minimum value is 1 and the maximum value is 255. The default is 5.

  **Example:**

  hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
  half-closed 0:20:0 dcd

**Step 5**

Decrement time-to-live (TTL) on packets that match the class: **set connection decrement-ttl**

This command, along with the *icmp unreachable* command, is required to allow a traceroute through the ASA that shows the ASA as one of the hops.

  **Example:**

  hostname(config)# class-map global-policy
  hostname(config-cmap)# match any
  hostname(config-cmap)# exit
  hostname(config)# policy-map global_policy
  hostname(config-pmap)# class global-policy
  hostname(config-pmap-c)# set connection decrement-ttl
  hostname(config-pmap-c)# exit
  hostname(config)# icmp unreachable rate-limit 50 burst-size 6

**Step 6**

Set advanced connection options.

Advanced options are special purpose configurations that are not needed under normal circumstances. You configure them with the **set connection advanced-options** command.

  • **set connection advanced-options tcp_map_name**—Customize TCP Normalizer behavior by applying a TCP map. For detailed information, see Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer), on page 445.

  • **set connection advanced-options tcp-state-bypass**—Implement TCP State Bypass. For detailed information, see Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass), on page 449.

  • **set connection advanced-options sctp-state-bypass**—Implement SCTP State Bypass to turn off SCTP stateful inspection. For more information, see SCTP Stateful Inspection, on page 395.

  • **set connection advanced-options flow-offload**—(ASA on the Firepower 4100/9300 chassis, FXOS 1.1.3 or later, only.) Implement flow offloading. Eligible traffic is offloaded to a super fast path, where the flows are switched in the NIC itself. You must also enter the *flow-offload enable* command, which is not part of the service policy.
Example:

hostname(config-pmap-c)# set connection advanced-options tcp_map1

Step 7

If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

service-policy policymap_name {global | interface interface_name}

Example:

hostname(config)# service-policy global_policy global

The global keyword applies the policy map to all interfaces, and interface applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

Example

The following example sets the connection limits and timeouts for all traffic:

hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 halff-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside

You can enter set connection commands with multiple parameters or you can enter each parameter as a separate command. The ASA combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50

The output of the show running-config policy-map command would display the result of the two commands in a single, combined command:

set connection conn-max 600 embryonic-conn-max 50

Monitoring Connections

You can use the following commands to monitor connections:

• show conn [detail]
Shows connection information. Detailed information uses flags to indicate special connection characteristics. For example, the “b” flag indicates traffic subject to TCP State Bypass.

- **show flow-offload \{info [detail] | cpu | flow [count | detail] | statistics\}**

  Shows information about the flow offloading, including general status information, CPU usage for offloading, offloaded flow counts and details, and offloaded flow statistics.

- **show service-policy**

  Shows service policy statistics, including Dead Connection Detection (DCD) statistics.

- **show threat-detection statistics top tcp-intercept [all | detail]**

  View the top 10 protected servers under attack. The `all` keyword shows the history data of all the traced servers. The `detail` keyword shows history sampling data. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.

### History for Connection Settings

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP state bypass</td>
<td>8.2(1)</td>
<td>This feature was introduced. The following command was introduced: <code>set connection advanced-options tcp-state-bypass</code>.</td>
</tr>
<tr>
<td>Connection timeout for all protocols</td>
<td>8.2(2)</td>
<td>The idle timeout was changed to apply to all protocols, not just TCP. The following command was modified: <code>set connection timeout</code>.</td>
</tr>
<tr>
<td>Timeout for connections using a backup static route</td>
<td>8.2(5)/8.4(2)</td>
<td>When multiple static routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value. We modified the following command: <code>timeout floating-conn</code>.</td>
</tr>
<tr>
<td>Configurable timeout for PAT xlate</td>
<td>8.4(3)</td>
<td>When a PAT xlate times out (by default after 30 seconds), and the ASA reuses the port for a new translation, some upstream routers might reject the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a value between 30 seconds and 5 minutes. We introduced the following command: <code>timeout pat-xlate</code>. This feature is not available in 8.5(1) or 8.6(1).</td>
</tr>
<tr>
<td>Increased maximum connection limits for service policy rules</td>
<td>9.0(1)</td>
<td>The maximum number of connections for service policy rules was increased from 65535 to 2000000. We modified the following commands: <code>set connection conn-max</code>, <code>set connection embryonic-conn-max</code>, <code>set connection per-client-embryonic-max</code>, <code>set connection per-client-max</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Decreased the half-closed timeout minimum value to 30 seconds</td>
<td>9.1(2)</td>
<td>The half-closed timeout minimum value for both the global timeout and connection timeout was lowered from 5 minutes to 30 seconds to provide better DoS protection. We modified the following commands: <code>set connection timeout half-closed</code>, <code>timeout half-closed</code>.</td>
</tr>
<tr>
<td>Connection holddown timeout for route convergence.</td>
<td>9.4(3) 9.6(2)</td>
<td>You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We added the following command: <code>timeout conn-holddown</code>.</td>
</tr>
<tr>
<td>SCTP idle timeout and SCTP state bypass</td>
<td>9.5(2)</td>
<td>You can set an idle timeout for SCTP connections. You can also enable SCTP state bypass to turn off SCTP stateful inspection on a class of traffic. We added or modified the following commands: <code>timeout sctp</code>, <code>set connection advanced-options sctp-state-bypass</code>.</td>
</tr>
<tr>
<td>Flow offload for the ASA on the Firepower 9300.</td>
<td>9.5(2.1)</td>
<td>You can identify flows that should be offloaded from the ASA and switched directly in the NIC (on the Firepower 9300). This provides improved performance for large data flows in data centers. This feature requires FXOS 1.1.3. We added or modified the following commands: <code>clear flow-offload</code>, <code>flow-offload enable</code>, <code>set-connection advanced-options flow-offload</code>, <code>show conn detail</code>, <code>show flow-offload</code>.</td>
</tr>
<tr>
<td>Flow offload support for the ASA on the Firepower 4100 series.</td>
<td>9.6(1)</td>
<td>You can identify flows that should be offloaded from the ASA and switched directly in the NIC for the Firepower 4100 series. This feature requires FXOS 1.1.4. There are no new commands or ASDM screens for this feature.</td>
</tr>
<tr>
<td>Flow offload support for multicast connections in transparent mode.</td>
<td>9.6(2)</td>
<td>You can now offload multicast connections to be switched directly in the NIC on transparent mode Firepower 4100 and 9300 series devices. Multicast offload is available for bridge groups that contain two and only two interfaces. There are no new commands or ASDM screens for this feature.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Changes in TCP option handling.                  | 9.6(2)            | You can now specify actions for the TCP MSS and MD5 options in a packet’s TCP header when configuring a TCP map. In addition, the default handling of the MSS, timestamp, window-size, and selective-ack options has changed. Previously, these options were allowed, even if there were more than one option of a given type in the header. Now, packets are dropped by default if they contain more than one option of a given type. For example, previously a packet with 2 timestamp options would be allowed, now it will be dropped. You can configure a TCP map to allow multiple options of the same type for MD5, MSS, selective-ack, timestamp, and window-size. For the MD5 option, the previous default was to clear the option, whereas the default now is to allow it. You can also drop packets that contain the MD5 option. For the MSS option, you can set the maximum segment size in the TCP map (per traffic class). The default for all other TCP options remains the same: they are cleared. We modified the following command: `timeout igp stale-route`.
| Stale route timeout for interior gateway protocols | 9.7(1)            | You can now configure the timeout for removing stale routes for interior gateway protocols such as OSPF. We added the following command: `timeout igp stale-route`.
| Global timeout for ICMP errors                   | 9.8(1)            | You can now set the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet. When this timeout is disabled (the default), and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors. We added the following command: `timeout icmp-error`.
| Default idle timeout for TCP state bypass        | 9.10(1)           | The default idle timeout for TCP state bypass connections is now 2 minutes instead of 1 hour.
CHAPTER 19

Quality of Service

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.

For the ASASM, we suggest performing QoS on the switch instead of the ASASM. Switches have more capability in this area. In general, QoS is best performed on the routers and switches in the network, which tend to have more extensive capabilities than the ASA.

The following topics describe how to apply QoS policies.

- About QoS, on page 465
- Guidelines for QoS, on page 467
- Configure QoS, on page 468
- Monitor QoS, on page 473
- Configuration Examples for Priority Queuing and Policing, on page 475
- History for QoS, on page 477

About QoS

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.

This section describes the QoS features available on the ASA.

Supported QoS Features

The ASA supports the following QoS features:

- Policing—To prevent classified traffic from hogging the network bandwidth, you can limit the maximum bandwidth used per class. See Policing, on page 466 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, a traffic policer. 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

Here are some definitions of these terms:

- 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 bytes per burst how much traffic can be sent within a given unit of time to not create scheduling concerns.
- 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 waits until the packet is discarded or marked down. 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.

Policing

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 class can take over the entire resource. When traffic exceeds the maximum rate, the ASA drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

Priority Queuing

LLQ priority queuing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic. Priority queuing uses an LLQ priority queue on an interface (see Configure the Priority Queue for an Interface, on page 469), 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 queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.

- 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 Priority Queuing, on page 466.
How QoS Features Interact

You can configure each of the QoS features alone if desired for the ASA. Often, though, you configure multiple QoS features on the ASA so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems. You can configure:

Priority queuing (for specific traffic) + Policing (for the rest of the traffic).

You cannot configure priority queuing and policing for the same set of traffic.

DSCP (DiffServ) Preservation

DSCP (DiffServ) markings are preserved on all traffic passing through the ASA. The ASA does not locally mark/remark any classified traffic. For example, you could key off the Expedited Forwarding (EF) DSCP bits of every packet to determine if it requires “priority” handling and have the ASA direct those packets to the LLQ.

Guidelines for QoS

Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

Firewall Mode Guidelines

Supported in routed firewall mode only. Does not support transparent firewall mode.

IPv6 Guidelines

Does not support IPv6.

Model Guidelines

- (ASA 5512-X through ASA 5555-X) Priority queuing is not supported on the Management 0/0 interface.
- (ASASM) Only policing is supported.

Additional Guidelines and Limitations

- QoS is applied unidirectionally; only traffic that enters (or exits, depending on the QoS feature) the interface to which you apply the policy map is affected.
- For priority traffic, you cannot use the class-default class map.
- For priority queuing, the priority queue must be configured for a physical interface or, for the ASASM, a VLAN.
- For policing, to-the-box traffic is not supported.
- For policing, traffic to and from a VPN tunnel bypasses interface policing.
- For policing, when you match a tunnel group class map, only outbound policing is supported.
Configure QoS

Use the following sequence to implement QoS on the ASA.

**Procedure**

- **Step 1** Determine the Queue and TX Ring Limits for a Priority Queue, on page 468.
- **Step 2** Configure the Priority Queue for an Interface, on page 469.
- **Step 3** Configure a Service Rule for Priority Queuing and Policing, on page 471.

Determine the Queue and TX Ring Limits for a Priority Queue

Use the following worksheets to determine the priority queue and TX ring limits.

**Queue Limit Worksheet**

The following worksheet shows how to calculate the priority queue size. 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 adjust the queue buffer size according to Configure the Priority Queue for an Interface, on page 469.

Tips on the worksheet:

- **Outbound bandwidth**—For example, DSL might have an uplink speed of 768 Kbps. Check with your provider.
- **Average packet size**—Determine this value from a codec or sampling size. For example, for VoIP over VPN, you might use 160 bytes. We recommend 256 bytes if you do not know what size to use.
- **Delay**—The delay depends on your application. For example, the recommended maximum delay for VoIP is 200 ms. We recommend 500 ms if you do not know what delay to use.

**Table 15: Queue Limit Worksheet**

<table>
<thead>
<tr>
<th></th>
<th>_________</th>
<th></th>
<th>__________</th>
<th>=</th>
<th>_________</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outbound bandwidth (Mbps or Kbps)</td>
<td>x</td>
<td>125</td>
<td>=</td>
<td># of bytes/ms</td>
</tr>
<tr>
<td></td>
<td>Kbps</td>
<td>x</td>
<td>.125</td>
<td>=</td>
<td># of bytes/ms</td>
</tr>
</tbody>
</table>
TX Ring Limit Worksheet

The following worksheet shows how to calculate the TX ring limit. This limit determines the maximum number of 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. This setting guarantees that the hardware-based transmit ring imposes a limited amount of extra latency for a high-priority packet.

Tips on the worksheet:

- Outbound bandwidth—For example, DSL might have an uplink speed of 768 Kbps. Check with your provider.

- Maximum packet size—Typically, the maximum size is 1538 bytes, or 1542 bytes for tagged Ethernet. If you allow jumbo frames (if supported for your platform), then the packet size might be larger.

- Delay—The delay depends on your application. For example, to control jitter for VoIP, you should use 20 ms.

Table 16: TX Ring Limit Worksheet

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outbound bandwidth (Mbps or Kbps)</td>
<td>x</td>
<td>125</td>
<td>=</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td># of bytes/ms</td>
</tr>
<tr>
<td></td>
<td>Kbps</td>
<td>x</td>
<td>0.125</td>
<td>=</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td># of bytes/ms</td>
</tr>
</tbody>
</table>

| 2 | # of bytes/ms from Step 1 | ÷ | Maximum packet size (bytes) | x | Delay (ms) | = | TX ring limit (# of packets) |

Configure the Priority Queue for an Interface

If you enable priority queuing 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.

Before you begin

- (ASASM) The ASASM does not support priority queuing.
- (ASA 5512-X through ASA 5555-X) Priority queuing is not supported on the Management 0/0 interface.

**Procedure**

**Step 1** Create the priority queue for the interface.

`priority-queue interface_name`

**Example:**

```
hostname(config)# priority-queue inside
```

The `interface_name` argument specifies the physical interface name on which you want to enable the priority queue, or for the ASASM, the VLAN interface name.

**Step 2** Change the size of the priority queues.

`queue-limit number_of_packets`

The default queue limit is 1024 packets. 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 the `queue-limit` command to increase the queue buffer size.

The upper limit of the range of values for the `queue-limit` command is determined dynamically at run time. To view this limit, enter `queue-limit ?` on the command line. 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.

**Example:**

```
hostname(config-priority-queue)# queue-limit 260
```

**Step 3** Specify the depth of the priority queues.

`tx-ring-limit number_of_packets`

The default tx-ring-limit is 511 packets. This command 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. This setting guarantees that the hardware-based transmit ring imposes a limited amount of extra latency for a high-priority packet.

The upper limit of the range of values for the `tx-ring-limit` command is determined dynamically at run time. To view this limit, enter `tx-ring-limit ?` on the command line. The key determinants are the memory needed to support the queues and the memory available on the device.

The `tx-ring-limit` that you specify affects both the higher priority low-latency queue and the best-effort queue.

**Example:**

```
hostname(config-priority-queue)# tx-ring-limit 3
```
Examples

The following example establishes a priority queue on interface “outside” (the GigabitEthernet0/1 interface), with the default queue-limit and tx-ring-limit:

hostname(config)# priority-queue outside

The following example establishes a priority queue on the interface “outside” (the GigabitEthernet0/1 interface), sets the queue-limit to 260 packets, and sets the tx-ring-limit to 3:

hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3

Configure a Service Rule for Priority Queuing and Policing

You can configure priority queuing and policing for different class maps within the same policy map. See How QoS Features Interact, on page 467 for information about valid QoS configurations.

Before you begin

- You cannot use the class-default class map for priority traffic.
- (ASASM) The ASASM only supports policing.
- For policing, to-the-box traffic is not supported.
- For policing, traffic to and from a VPN tunnel bypasses interface policing.
- For policing, when you match a tunnel group class map, only outbound policing is supported.
- For priority traffic, identify only latency-sensitive traffic.
- For policing traffic, you can choose to police all other traffic, or you can limit the traffic to certain types.

Procedure

Step 1

Create an L3/L4 class map to identify the traffic for which you want to perform priority queuing.

```
class-map name
match parameter
```

Example:

```
hostname(config)# class-map priority_traffic
hostname(config-cmap)# match access-list priority
```

See Create a Layer 3/4 Class Map for Through Traffic, on page 295 for more information.
Step 2 
Create an L3/L4 class map to identify the traffic for which you want to perform priority policing.

```plaintext
class-map name
match parameter
```

Example:
```
hostname(config)# class-map policing_traffic
hostname(config-cmap)# match access-list policing
```

Tip If you use an ACL for traffic matching, policing is applied in the direction specified in the ACL only. That is, traffic going from the source to the destination is policed, but not the reverse.

Step 3 
Add or edit a policy map: `policy-map name`

Example:
```
hostname(config)# policy-map QoS_policy
```

Step 4 
Identify the class map you created for prioritized traffic and configure priority queuing for the class.

```plaintext
class priority_map_name
priority
```

Example:
```
hostname(config-pmap)# class priority_class
hostname(config-pmap-c)# priority
```

Step 5 
Identify the class map you created for policed traffic: `class name`

Example:
```
hostname(config-pmap)# class policing_class
```

Step 6 
Configure policing for the class.

```plaintext
policy {output | input} conform-rate [conform-burst] [conform-action [drop | transmit]] [exceed-action [drop | transmit]]
```

The options are:

- **output**—Enables policing of traffic flowing in the output direction.
- **input**—Enables policing of traffic flowing in the input direction.
- **conform-rate**—Sets the rate limit for this traffic class; between 8000 and 2000000000 bits per second.
- **conform-burst**—Specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512000000 bytes.
- **conform-action**—Sets the action to take when the rate is less than the `conform_burst` value. You can drop or transmit the packet.
Monitor QoS

The following topics explain how to monitor QoS.

QoS Police Statistics

To view the QoS statistics for traffic policing, use the show service-policy police command.

hostname# show service-policy police

Global policy:
Service-policy: global_fw_policy

Interface outside:
Service-policy: qos
Class-map: browse
  police Interface outside:
  cir 56000 bps, bc 10500 bytes
  conformed 10065 packets, 12621510 bytes; actions: transmit
exceeded 499 packets, 625146 bytes; actions: drop
  conformed 5600 bps, exceed 5016 bps
Class-map: cmap2
  police Interface outside:
  cir 200000 bps, bc 37500 bytes
  conformed 17179 packets, 20614800 bytes; actions: transmit
  exceeded 617 packets, 770718 bytes; actions: drop
  conformed 198785 bps, exceed 2303 bps
QoS Priority Statistics

To view statistics for service policies implementing the priority command, use the `show service-policy priority` command.

```
hostname# show service-policy priority
Global policy:
  Service-policy: global_fw_policy
Interface outside:
  Service-policy: qos
    Class-map: TG1-voice
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 9383
```

“Aggregate drop” denotes the aggregated drop in this interface; “aggregate transmit” denotes the aggregated number of transmitted packets in this interface.

QoS Priority Queue Statistics

To display the priority-queue statistics for an interface, use the `show priority-queue statistics` command. The results show the statistics for both the best-effort (BE) queue and the low-latency queue (LLQ). The following example shows the use of the `show priority-queue statistics` command for the interface named test.

```
hostname# show priority-queue statistics test
Priority-Queue Statistics interface test
  Queue Type          = BE
  Packets Dropped    = 0
  Packets Transmit   = 0
  Packets Enqueued   = 0
  Current Q Length   = 0
  Max Q Length       = 0

  Queue Type          = LLQ
  Packets Dropped    = 0
  Packets Transmit   = 0
  Packets Enqueued   = 0
  Current Q Length   = 0
  Max Q Length       = 0
hostname#
```

In this statistical report:

- “Packets Dropped” denotes the overall number of packets that have been dropped in this queue.
- “Packets Transmit” denotes the overall number of packets that have been transmitted in this queue.
- “Packets Enqueued” denotes the overall number of packets that have been queued in this queue.
- “Current Q Length” denotes the current depth of this queue.
- “Max Q Length” denotes the maximum depth that ever occurred in this queue.
Configuration Examples for Priority Queuing and Policing

The following sections provide examples of configuring priority queuing and policing.

Class Map Examples for VPN Traffic

In the following example, the `class-map` command classifies all non-tunneled TCP traffic, using an ACL named `tcp_traffic`:

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

In the following example, other, more specific match criteria are used for classifying traffic for specific, security-related tunnel groups. These specific match criteria stipulate that a match on tunnel-group (in this case, the previously-defined Tunnel-Group-1) is required as the first match characteristic to classify traffic for a specific tunnel, and it allows for an additional match line to classify the traffic (IP differential services code point, expedited forwarding).

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

In the following example, the `class-map` command classifies both tunneled and non-tunneled traffic according to the traffic type:

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0 192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L
hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled
hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

The following example shows a way of policing traffic within a tunnel, provided the classed traffic is not specified as a tunnel, but does go *through* the tunnel. In this example, 192.168.10.10 is the address of the host machine on the private side of the remote tunnel, and the ACL is named “host-over-L2L”. By creating a class-map (named “host-specific”), you can then police the “host-specific” class before the LAN-to-LAN connection.
policies the tunnel. In this example, the “host-specific” traffic is rate-limited before the tunnel, then the tunnel is rate-limited:

hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l

Priority and Policing Example

The following example builds on the configuration developed in the previous section. As in the previous example, there are two named class-maps: tcp_traffic and TG1-voice.

hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address

Adding a third class map provides a basis for defining a tunneled and non-tunneled QoS policy, as follows, which creates a simple QoS policy for tunneled and non-tunneled traffic, assigning packets of the class TG1-voice to the low latency queue and setting rate limits on the tcp_traffic and TG1-best-effort traffic flows.

In this example, the maximum rate for traffic of the tcp_traffic class is 56,000 bits/second and a maximum burst size of 10,500 bytes per second. For the TC1-BestEffort class, the maximum rate is 200,000 bits/second, with a maximum burst of 37,500 bytes/second. Traffic in the TC1-voice class has no policed maximum speed or burst rate because it belongs to a priority class.

hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500
hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500
hostname(config-pmap-c)# service-policy qos global
## History for QoS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority queuing and policing</td>
<td>7.0(1)</td>
<td>We introduced QoS priority queuing and policing. We introduced the following commands: priority-queue, queue-limit, tx-ring-limit, priority, police, show priority-queue statistics, show service-policy police, show service-policy priority, show running-config priority-queue, clear configure priority-queue.</td>
</tr>
<tr>
<td>Shaping and hierarchical priority queuing</td>
<td>7.2(4)/8.0(4)</td>
<td>We introduced QoS shaping and hierarchical priority queuing. We introduced the following commands: shape, show service-policy shape.</td>
</tr>
<tr>
<td>Ten Gigabit Ethernet support for a standard priority queue on the ASA 5585-X</td>
<td>8.2(3)/8.4(1)</td>
<td>We added support for a standard priority queue on Ten Gigabit Ethernet interfaces for the ASA 5585-X.</td>
</tr>
</tbody>
</table>
CHAPTER 20

Threat Detection

The following topics describe how to configure threat detection statistics and scanning threat detection.

- Detecting Threats, on page 479
- Guidelines for Threat Detection, on page 481
- Defaults for Threat Detection, on page 482
- Configure Threat Detection, on page 483
- Monitoring Threat Detection, on page 486
- Examples for Threat Detection, on page 492
- History for Threat Detection, on page 493

Detecting Threats

Threat detection on the ASA provides a front-line defense against attacks. Threat detection works at Layer 3 and 4 to develop a baseline for traffic on the device, analyzing packet drop statistics and accumulating "top" reports based on traffic patterns. In comparison, a module that provides IPS or Next Generation IPS services identifies and mitigates attack vectors up to Layer 7 on traffic the ASA permitted, and cannot see the traffic dropped already by the ASA. Thus, threat detection and IPS can work together to provide a more comprehensive threat defense.

Threat detection consists of the following elements:

- Different levels of statistics gathering for various threats.

Threat detection statistics can help you manage threats to your ASA; for example, if you enable scanning threat detection, then viewing statistics can help you analyze the threat. You can configure two types of threat detection statistics:

- Basic threat detection statistics—Includes information about attack activity for the system as a whole. Basic threat detection statistics are enabled by default and have no performance impact.

- Advanced threat detection statistics—Tracks activity at an object level, so the ASA can report activity for individual hosts, ports, protocols, or ACLs. Advanced threat detection statistics can have a major performance impact, depending on the statistics gathered, so only the ACL statistics are enabled by default.

- Scanning threat detection, which determines when a host is performing a scan. You can optionally shun any hosts determined to be a scanning threat.
Basic Threat Detection Statistics

Using basic threat detection statistics, the ASA monitors the rate of dropped packets and security events due to the following reasons:

- Denial by ACLs.
- 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 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 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 UDP session with no return data attack detected.

When the ASA detects a threat, it immediately sends a system log message (733100). The ASA 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 1/30th of the average rate interval or 10 seconds, whichever is higher. For each received event, the ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA sends two separate system messages, with a maximum of one message for each rate type per burst period.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Advanced Threat Detection Statistics

Advanced threat detection statistics show both allowed and dropped traffic rates for individual objects such as hosts, ports, protocols, or ACLs.

⚠️ Caution

Enabling advanced statistics can affect the ASA performance, depending on the type of statistics enabled. Enabling host statistics affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Port statistics, however, has modest impact.
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, ASA threat detection scanning 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.

If the scanning threat rate is exceeded, then the ASA sends a syslog message (733101), and optionally shuns the attacker. The ASA 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 1/30th 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 ASA 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.

The following table lists the default rate limits for scanning threat detection.

<table>
<thead>
<tr>
<th>Average Rate</th>
<th>Burst Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 drops/sec over the last 600 seconds.</td>
<td>10 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td>5 drops/sec over the last 3600 seconds.</td>
<td>10 drops/sec over the last 120 second period.</td>
</tr>
</tbody>
</table>

The scanning threat detection feature can affect the ASA performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

Guidelines for Threat Detection

Security Context Guidelines

Except for advanced threat statistics, threat detection is supported in single mode only. In Multiple mode, TCP Intercept statistics are the only statistic supported.

Types of Traffic Monitored

- Only through-the-box traffic is monitored; to-the-box traffic is not included in threat detection.
- Traffic that is denied by an ACL does not trigger scanning threat detection; only traffic that is allowed through the ASA and that creates a flow is affected by scanning threat detection.
## Defaults for Threat Detection

Basic threat detection statistics are enabled by default.

The following table lists the default settings. You can view all these default settings using the `show running-config all threat-detection` command.

For advanced statistics, by default, statistics for ACLs are enabled.

### Table 18: Basic Threat Detection Default Settings

<table>
<thead>
<tr>
<th>Packet Drop Reason</th>
<th>Trigger Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DoS attack detected</strong></td>
<td><strong>Average Rate</strong>: 100 drops/sec over the last 600 seconds. <strong>Burst Rate</strong>: 400 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td><strong>Bad packet format</strong></td>
<td><strong>Average Rate</strong>: 80 drops/sec over the last 3600 seconds. <strong>Burst Rate</strong>: 320 drops/sec over the last 120 second period.</td>
</tr>
<tr>
<td><strong>Connection limits exceeded</strong></td>
<td><strong>Average Rate</strong>: 10 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td><strong>Suspicious ICMP packets detected</strong></td>
<td><strong>Average Rate</strong>: 5 drops/sec over the last 600 seconds.</td>
</tr>
<tr>
<td><strong>Scanning attack detected</strong></td>
<td><strong>Average Rate</strong>: 4 drops/sec over the last 3600 seconds. <strong>Burst Rate</strong>: 8 drops/sec over the last 120 second period.</td>
</tr>
<tr>
<td><strong>Incomplete session detected such as TCP SYN attack detected or UDP session with no return data attack detected (combined)</strong></td>
<td><strong>Average Rate</strong>: 100 drops/sec over the last 600 seconds. <strong>Burst Rate</strong>: 200 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td><strong>Denial by ACLs</strong></td>
<td><strong>Average Rate</strong>: 80 drops/sec over the last 3600 seconds. <strong>Burst Rate</strong>: 160 drops/sec over the last 120 second period.</td>
</tr>
<tr>
<td><strong>Basic firewall checks failed</strong></td>
<td><strong>Average Rate</strong>: 400 drops/sec over the last 600 seconds. <strong>Burst Rate</strong>: 800 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td><strong>Packets failed application inspection</strong></td>
<td><strong>Average Rate</strong>: 320 drops/sec over the last 3600 seconds. <strong>Burst Rate</strong>: 640 drops/sec over the last 120 second period.</td>
</tr>
<tr>
<td><strong>Interface overload</strong></td>
<td><strong>Average Rate</strong>: 2000 drops/sec over the last 600 seconds. <strong>Burst Rate</strong>: 8000 drops/sec over the last 20 second period.</td>
</tr>
<tr>
<td></td>
<td><strong>Average Rate</strong>: 1600 drops/sec over the last 3600 seconds. <strong>Burst Rate</strong>: 6400 drops/sec over the last 120 second period.</td>
</tr>
</tbody>
</table>
Configure Threat Detection

Basic threat detection statistics are enabled by default, and might be the only threat detection service that you need. Use the following procedure if you want to implement additional threat detection services.

Procedure

Step 1
Configure Basic Threat Detection Statistics, on page 483.
Basic threat detection statistics include activity that might be related to an attack, such as a DoS attack.

Step 2
Configure Advanced Threat Detection Statistics, on page 484.

Step 3
Configure Scanning Threat Detection, on page 485.

Configure Basic Threat Detection Statistics

Basic threat detection statistics is enabled by default. You can disable it, or turn it on again if you disable it.

Procedure

Step 1
Enable basic threat detection statistics (if you previously disabled it).

threat-detection basic-threat

Example:

hostname(config)# threat-detection basic-threat

Basic threat detection is enabled by default. Use no threat-detection basic-threat to disable it.

Step 2
(Optional) Change the default settings for one or more type of event.

threat-detection rate {acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack} rate-interval rate_interval average-rate av_rate burst-rate burst_rate

For a description of each event type, see Basic Threat Detection Statistics.

When you use this command with the scanning-threat keyword, it is also used in the scanning threat detection. If you do not configure basic threat detection, you can still use this command with the scanning-threat keyword to configure the rate limits for scanning threat detection.

You can configure up to three different rate intervals for each event type.

Example:

hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate
Configure Advanced Threat Detection Statistics

You can configure the ASA to collect extensive statistics. By default, statistics for ACLs are enabled. To enable other statistics, perform the following steps.

Procedure

Step 1  
(Optional) Enable all statistics.

`threat-detection statistics`

To enable only certain statistics, enter this command for each statistic type (shown later in this procedure), and do not also enter the command without any options. You can enter `threat-detection statistics` (without any options) and then customize certain statistics by entering the command with statistics-specific options (for example, `threat-detection statistics host number-of-rate 2`). If you enter `threat-detection statistics` (without any options) and then enter a command for specific statistics, but without any statistic-specific options, then that command has no effect because it is already enabled.

If you enter the `no` form of this command, it removes all `threat-detection statistics` commands, including the `threat-detection statistics access-list` command, which is enabled by default.

Example:

```
hostname(config)# threat-detection statistics
```

Step 2  
(Optional) Enable statistics for ACLs (if they were disabled previously).

`threat-detection statistics access-list`

Statistics for ACLs are enabled by default. ACL statistics are only displayed using the `show threat-detection top access-list` command.

Example:

```
hostname(config)# threat-detection statistics access-list
```

Step 3  
(Optional) Configure statistics for hosts (`host` keyword), TCP and UDP ports (`port` keyword), or non-TCP/UDP IP protocols (`protocol` keyword).

`threat-detection statistics {host | port | protocol} [number-of-rate {1 | 2 | 3}]`

The `number-of-rate` keyword sets the number of rate intervals maintained for statistics. The default number of rate intervals is 1, which keeps the memory usage low. To view more rate intervals, set the value to 2 or 3. For example, if you set the value to 3, then you view data for the last 1 hour, 8 hours, and 24 hours. If you set this keyword to 1 (the default), then only the shortest rate interval statistics are maintained. If you set the value to 2, then the two shortest intervals are maintained.

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.
Example:

hostname(config)# threat-detection statistics host number-of-rate 2
hostname(config)# threat-detection statistics port number-of-rate 2
hostname(config)# threat-detection statistics protocol number-of-rate 3

Step 4  (Optional) Configure statistics for attacks intercepted by TCP Intercept.

threat-detection statistics tcp-intercept [rate-interval minutes] [burst-rate attacks_per_sec] [average-rate attacks_per_sec]

Where:

- **rate-interval** sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the ASA samples the number of attacks 30 times.
- **burst-rate** sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
- **average-rate** sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.

To enable TCP Intercept, see Protect Servers from a SYN Flood DoS Attack (TCP Intercept), on page 443.

**Note**  This command is available in multiple context mode, unlike the other threat-detection commands.

Example:

hostname(config)# threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600

---

Configure Scanning Threat Detection

You can configure scanning threat detection to identify attackers and optionally shun them.

**Procedure**

**Step 1**  Enable scanning threat detection.

threat-detection scanning-threat [shun [except {ip-address ip_address mask | object-group network_object_group_id}]]

By default, the system log message 733101 is generated when a host is identified as an attacker. Enter this command multiple times to identify multiple IP addresses or network object groups to exempt from shunning.

**Example:**

hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
Step 2  
(Optional) Set the duration of the shun for attacking hosts.

```
threat-detection scanning-threat shun duration seconds
```

**Example:**

hostname(config)# threat-detection scanning-threat shun duration 2000

Step 3  
(Optional) Change the default event limit for when the ASA identifies a host as an attacker or as a target.

```
threat-detection rate scanning-threat rate-interval rate_interval average-rate avg_rate burst-rate burst_rate
```

If you already configured this command as part of the basic threat detection configuration, then those settings are shared with the scanning threat detection feature; you cannot configure separate rates for basic and scanning threat detection. If you do not set the rates using this command, the default values are used for both the scanning threat detection feature and the basic threat detection feature. You can configure up to three different rate intervals by entering separate commands.

**Example:**

hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20

---

**Monitoring Threat Detection**

The following topics explain how to monitor threat detection and view traffic statistics.

**Monitoring Basic Threat Detection Statistics**

To display basic threat detection statistics, use the following command:

```
show threat-detection rate [min-display-rate min_display_rate] [acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack]
```

The *min-display-rate* *min_display_rate* argument limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.

The other arguments let you limit the display to specific categories. For a description of each event type, see Basic Threat Detection Statistics, on page 480.

The output shows the average rate in events/sec over two fixed time periods: the last 10 minutes and the last 1 hour. It also shows: the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger; the number of times the rates were exceeded (triggered); and the total number of events over the time periods.

The ASA stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the *show* command at 3:00:25, then the last 5 seconds are not included in the output.
The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

You can clear statistics using the clear threat-detection rate command.

The following is sample output from the show threat-detection rate command:

```
hostname# show threat-detection rate

Average(eps) Current(eps) Trigger Total events
10-min ACL drop: 0 0 0 16
1-hour ACL drop: 0 0 0 112
1-hour SYN attck: 5 0 2 21438
10-min Scanning: 0 0 29 193
1-hour Scanning: 106 0 10 384776
1-hour Bad pkts: 76 0 2 274690
10-min Firewall: 76 0 3 22
1-hour Firewall: 76 0 2 274844
10-min DoS attck: 0 0 0 6
1-hour DoS attck: 0 0 0 42
10-min Interface: 0 0 0 204
1-hour Interface: 88 0 0 318225
```

**Monitoring Advanced Threat Detection Statistics**

To monitor advanced threat detection statistics, use the commands shown in the following table. The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the show command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>top</code> `[[access-list</td>
<td>host</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>top</code> `access-list [rate-1</td>
<td>rate-2</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>top</code> `host [rate-1</td>
<td>rate-2</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>top</code> `port-protocol [rate-1</td>
<td>rate-2</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>top</code> <code>tcp-intercept [all] detail]</code></td>
<td>To view TCP Intercept statistics, use the <code>tcp-intercept</code> keyword. The display includes the top 10 protected servers under attack. The <code>all</code> keyword shows the history data of all the traced servers. The <code>detail</code> keyword shows history sampling data. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate]</code> <code>host</code> <code>[ip_address [mask]]</code></td>
<td>Displays statistics for all hosts or for a specific host or subnet.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> <code>min_display_rate] port [start_port[-end_port]]</code></td>
<td>Displays statistics for all ports or for a specific port or range of ports.</td>
</tr>
<tr>
<td><code>show threat-detection statistics [min-display-rate</code> `min_display_rate] protocol [protocol_number</td>
<td>protocol]`</td>
</tr>
<tr>
<td></td>
<td>The <code>protocol_number</code> argument is an integer between 0 and 255.</td>
</tr>
<tr>
<td></td>
<td>The <code>protocol</code> argument can be one of ah, eigrp, esp, gre, icmp, icmp6,</td>
</tr>
<tr>
<td></td>
<td>igmp, igrp, ip, ipinip, ipsec, nos, ospf, pcp, pim, ppp, snp, tcp, udp.</td>
</tr>
</tbody>
</table>

### Evaluating Host Threat Detection Statistics

The following is sample output from the `show threat-detection statistics host` command:

```
hostname# show threat-detection statistics host

Table: Average (eps) Current (eps) Trigger Total events
Host: 10.0.0.1:
1-hour Sent byte: 2938 0 0 10580308
8-hour Sent byte: 367 0 0 10580308
24-hour Sent byte: 122 0 0 10580308
1-hour Sent pkts: 28 0 0 104043
8-hour Sent pkts: 3 0 0 104043
24-hour Sent pkts: 1 0 0 104043
20-min Sent drop: 9 0 1 10851
1-hour Sent drop: 3 0 1 10851
1-hour Recv byte: 2697 0 0 9712670
8-hour Recv byte: 337 0 0 9712670
24-hour Recv byte: 112 0 0 9712670
1-hour Recv pkts: 29 0 0 104846
8-hour Recv pkts: 3 0 0 104846
24-hour Recv pkts: 1 0 0 104846
20-min Recv drop: 14 0 1 50567
1-hour Recv drop: 0 0 0 4
1-hour Sent byte: 0 0 0 614
8-hour Sent byte: 0 0 0 614
24-hour Sent byte: 0 0 0 614
1-hour Sent pkts: 0 0 0 6
8-hour Sent pkts: 0 0 0 6
24-hour Sent pkts: 0 0 0 6
20-min Sent drop: 0 0 0 4
1-hour Sent drop: 0 0 0 4
1-hour Recv byte: 0 0 0 706
8-hour Recv byte: 0 0 0 706
24-hour Recv byte: 0 0 0 706
1-hour Recv pkts: 0 0 0 7
```

The following table explains the output.

**Table 19: show threat-detection statistics host**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The host IP address.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tot-ses</td>
<td>The total number of sessions for this host since it was added to the database.</td>
</tr>
<tr>
<td>act-ses</td>
<td>The total number of active sessions that the host is currently involved in.</td>
</tr>
<tr>
<td>fw-drop</td>
<td>The number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including ACL denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and UDP session with no return data attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.</td>
</tr>
<tr>
<td>insp-drop</td>
<td>The number of packets dropped because they failed application inspection.</td>
</tr>
<tr>
<td>null-ses</td>
<td>The number of null sessions, which are TCP SYN sessions that did not complete within the 3-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.</td>
</tr>
<tr>
<td>bad-acc</td>
<td>The number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see the null-ses field description), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.</td>
</tr>
<tr>
<td>Average(eps)</td>
<td>The average rate in events/sec over each time period. The ASA stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the <code>show</code> command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.</td>
</tr>
<tr>
<td>Current(eps)</td>
<td>The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00.</td>
</tr>
<tr>
<td>Trigger</td>
<td>The number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Total events | The total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

### 20-min, 1-hour, 8-hour, and 24-hour
Statistics for these fixed rate intervals. For each interval:
- **Sent byte**—The number of successful bytes sent from the host.
- **Sent pkts**—The number of successful packets sent from the host.
- **Sent drop**—The number of packets sent from the host that were dropped because they were part of a scanning attack.
- **Recv byte**—The number of successful bytes received by the host.
- **Recv pkts**—The number of successful packets received by the host.
- **Recv drop**—the number of packets received by the host that were dropped because they were part of a scanning attack.

---

**Monitoring Shunned Hosts, Attackers, and Targets**

To monitor and manage shunned hosts and attackers and targets, use the following commands:

- **show threat-detection shun**
  Displays the hosts that are currently shunned. For example:

  hostname# show threat-detection shun

  Shunned Host List:
  (outside) src-ip=10.0.0.13 255.255.255.255
  (inside) src-ip=10.0.0.13 255.255.255.255

- **clear threat-detection shun [ip_address [mask]]**
  Releases a host from being shunned. If you do not specify an IP address, all hosts are cleared from the shun list.
  For example, to release the host at 10.1.1.6, enter the following command:

  hostname# clear threat-detection shun 10.1.1.6

- **show threat-detection scanning-threat [attacker | target]**
  Displays hosts that the ASA decides are attackers (including hosts on the shun list), and displays the hosts that are the target of an attack. If you do not enter an option, both attackers and target hosts are displayed. For example:
hostname# show threat-detection scanning-threat

Latest Target Host & Subnet List:
192.168.1.0 (l2l)
192.168.1.249 (l2l)

Latest Attacker Host & Subnet List:
192.168.10.234 (outside)
192.168.10.0 (outside)
192.168.10.2 (outside)
192.168.10.3 (outside)
192.168.10.4 (outside)
192.168.10.5 (outside)
192.168.10.6 (outside)
192.168.10.7 (outside)
192.168.10.8 (outside)
192.168.10.9 (outside)

---

Examples for Threat Detection

The following example configures basic threat detection statistics, and changes the DoS attack rate settings. All advanced threat detection statistics are enabled, with the host statistics number of rate intervals lowered to 2. The TCP Intercept rate interval is also customized. Scanning threat detection is enabled with automatic shunning for all addresses except 10.1.1.0/24. The scanning threat rate intervals are customized.

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```
## History for Threat Detection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic and advanced threat detection statistics, scanning threat detection</td>
<td>8.0(2)</td>
<td>Basic and advanced threat detection statistics, scanning threat detection was introduced. The following commands were introduced: threat-detection basic-threat, threat-detection rate, show threat-detection rate, clear threat-detection rate, threat-detection statistics, show threat-detection statistics, threat-detection scanning-threat, threat-detection rate scanning-threat, show threat-detection scanning-threat, show threat-detection shun, clear threat-detection shun.</td>
</tr>
<tr>
<td>Shun duration</td>
<td>8.0(4)/8.1(2)</td>
<td>You can now set the shun duration. The following command was introduced: threat-detection scanning-threat shun duration.</td>
</tr>
<tr>
<td>TCP Intercept statistics</td>
<td>8.0(4)/8.1(2)</td>
<td>TCP Intercept statistics were introduced. The following commands were modified or introduced: threat-detection statistics tcp-intercept, show threat-detection statistics top tcp-intercept, clear threat-detection statistics.</td>
</tr>
<tr>
<td>Customize host statistics rate intervals</td>
<td>8.1(2)</td>
<td>You can now customize the number of rate intervals for which statistics are collected. The default number of rates was changed from 3 to 1. The following command was modified: threat-detection statistics host number-of-rates.</td>
</tr>
<tr>
<td>Burst rate interval changed to 1/30th of the average rate.</td>
<td>8.2(1)</td>
<td>In earlier releases, the burst rate interval was 1/60th of the average rate. To maximize memory usage, the sampling interval was reduced to 30 times during the average rate.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Customize port and protocol statistics rate intervals</td>
<td>8.3(1)</td>
<td>You can now customize the number of rate intervals for which statistics are collected. The default number of rates was changed from 3 to 1. The following commands were modified: <strong>threat-detection statistics port number-of-rates</strong>, <strong>threat-detection statistics protocol number-of-rates</strong>.</td>
</tr>
<tr>
<td>Improved memory usage</td>
<td>8.3(1)</td>
<td>The memory usage for threat detection was improved. The following command was introduced: <strong>show threat-detection memory</strong>.</td>
</tr>
</tbody>
</table>