Cisco ASA Series Firewall ASDM Configuration Guide

Software Version 7.3

Released: July 24, 2014
Updated: February 18, 2015

Cisco Systems, Inc.
www.cisco.com

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

- Document Objectives, page iii
- Related Documentation, page iii
- Conventions, page iv
- Obtaining Documentation and Submitting a Service Request, page iv

Document Objectives

The purpose of this guide is to help you configure the firewall features for Cisco ASA series using the Adaptive Security Device Manager (ASDM). This guide does not cover every feature, but describes only the most common configuration scenarios.

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

Note

ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Please refer to the feature history table for each chapter to determine when features were added. For the minimum supported version of ASDM for each ASA version, see Cisco ASA Series Compatibility.

Related Documentation

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

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold font</strong></td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[   ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier font</strong>.</td>
</tr>
<tr>
<td><strong>courier bold font</strong></td>
<td>Commands and keywords and user-entered text appear in <strong>bold courier font</strong>.</td>
</tr>
<tr>
<td><strong>courier italic font</strong></td>
<td>Arguments for which you supply values are in <strong>courier italic font</strong>.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[   ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

Means reader take note.

**Tip**

Means the following information will help you solve a problem.

**Caution**

Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
PART 1

Service Policies and Access Control
Service Policy

Updated: February 18, 2015

Service policies 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, page 1-1
- Guidelines for Service Policies, page 1-8
- Defaults for Service Policies, page 1-9
- Configure Service Policies, page 1-10
- History for Service Policies, page 1-16

About Service Policies

The following topics describe how service policies work.

- The Components of a Service Policy, page 1-1
- Features Configured with Service Policies, page 1-4
- Feature Directionality, page 1-4
- Feature Matching Within a Service Policy, page 1-5
- Order in Which Multiple Feature Actions are Applied, page 1-6
- Incompatibility of Certain Feature Actions, page 1-7
- Feature Matching for Multiple Service Policies, page 1-7

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.
   a. The `class` command defines the traffic matching criteria for the rule.
   b. 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:

- 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 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.
  policy-map type inspect sip sip-high
  parameters
  rtp-conformance enforce-payloadtype
  no traffic-non-sip
  software-version action mask log
  ```
Chapter 1  Service Policy

About Service Policies

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_1

: 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

: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
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 1-1 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>• Chapter 7, “Getting Started with Application Layer Protocol Inspection.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Chapter 8, “Inspection of Basic Internet Protocols.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Chapter 9, “Inspection for Voice and Video Protocols.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Chapter 10, “Inspection of Database and Directory Protocols.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Chapter 11, “Inspection for Management Application Protocols.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Chapter 15, “ASA and Cisco Cloud Web Security.”</td>
</tr>
<tr>
<td>ASA IPS</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 19, “ASA IPS Module.”</td>
</tr>
<tr>
<td>ASA CX</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 18, “ASA CX Module.”</td>
</tr>
<tr>
<td>ASA FirePOWER (ASA SFR)</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 16, “ASA FirePOWER (SFR) Module.”</td>
</tr>
<tr>
<td>NetFlow Secure Event Logging filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>See the general operations configuration guide.</td>
</tr>
<tr>
<td>QoS input and output policing</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 13, “Quality of Service.”</td>
</tr>
<tr>
<td>QoS standard priority queue</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 13, “Quality of Service.”</td>
</tr>
<tr>
<td>TCP and UDP connection limits and timeouts, and TCP sequence number randomization</td>
<td>Yes</td>
<td>Yes</td>
<td>Chapter 12, “Connection Settings.”</td>
</tr>
<tr>
<td>TCP normalization</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 12, “Connection Settings.”</td>
</tr>
<tr>
<td>TCP state bypass</td>
<td>Yes</td>
<td>No</td>
<td>Chapter 12, “Connection Settings.”</td>
</tr>
<tr>
<td>User statistics for Identity Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>See the user-statistics command in the command reference.</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.
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 1-2 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 CSC</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>
<tr>
<td>QoS standard priority queue</td>
<td>Egress</td>
<td>Egress</td>
</tr>
<tr>
<td>TCP and UDP connection limits and timeouts, and TCP sequence number randomization</td>
<td>Bidirectional</td>
<td>Ingress</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>

### Feature Matching Within a Service Policy

A packet matches rules in a policy for a given interface according to the following rules:

1. A packet can match only one rule for an interface for each feature type.
2. When the packet matches a rule for a feature type, the ASA does not attempt to match it to any subsequent rules for that feature type.
3. If the packet matches a subsequent rule for a different feature type, however, then the ASA also applies the actions for the subsequent rule, if supported. See Incompatibility of Certain Feature Actions, page 1-7 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 rule for connection limits, and also matches a rule for an application inspection, then both actions are applied.
- If a packet matches a rule for HTTP inspection, but also matches another rule that includes HTTP inspection, then the second rule actions are not applied.
- If a packet matches a rule for HTTP inspection, but also matches another rule that includes FTP inspection, then the second rule actions are not applied because HTTP and FTP inspections cannot be combined.
- If a packet matches a rule for HTTP inspection, but also matches another rule that includes IPv6 inspection, then both actions are applied because the IPv6 inspection can be combined with any other type of inspection.

Order in Which Multiple Feature Actions are Applied

The order in which different types of actions in a service policy are performed is independent of the order in which the actions appear in the table.

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.
3. ASA CSC
4. Application inspections that can be combined with other inspections:
   a. IPv6
   b. IP options
   c. WAAS
5. Application inspections that cannot be combined with other inspections. See Incompatibility of Certain Feature Actions, page 1-7 for more information.
6. ASA IPS
7. ASA CX
8. ASA FirePOWER (ASA SFR)
9. QoS output policing
10. QoS standard priority queue

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.

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, page 1-6.
- 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.

Note

The Default Inspection Traffic traffic class, 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).

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

IPv6 Guidelines
Supports IPv6 for the following features:

- Application inspection for DNS, FTP, HTTP, ICMP, ScanSafe, SIP, SMTP, IPsec-pass-thru, and IPv6.
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow Secure Event Logging filtering
- 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. See Default Class Maps (Traffic Classes), page 1-9.

Service Policy Guidelines

- Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with FTP inspection, and an interface policy with TCP 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 interface policy with FTP inspection, then only the interface policy FTP inspection is applied to that interface.

- 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, page 1-9
- Default Class Maps (Traffic Classes), page 1-9

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

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
Configure Service Policies

Configuring a service policy consists of adding one or more service policy rules per interface or for the global policy. ASDM uses a wizard to take you through the process of creating a service policy. For each rule, you identify the following elements:

1. The interface to which you want to apply the rule, or the global policy.
2. The traffic to which you want to apply actions. You can identify Layer 3 and 4 traffic.
3. The actions to apply to the traffic class. You can apply multiple non-conflicting actions for each traffic class.

After you create a policy, you can add rules, move, edit, or delete rules or policies. The following topics explain how to configure service policies.

- Add a Service Policy Rule for Through Traffic, page 1-10
- Add a Service Policy Rule for Management Traffic, page 1-13
- Manage the Order of Service Policy Rules, page 1-15

Add a Service Policy Rule for Through Traffic

To add a service policy rule for through traffic, use the Add Service Policy Rule wizard. You will be asked to choose the scope of the policy, for a specific interface or global:

- Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with FTP inspection, and an interface policy with TCP connection limits, then both FTP inspection and TCP connection limits are applied to the interface. However, if you have a global policy with FTP inspection, and an interface policy with FTP inspection, then only the interface policy FTP inspection is applied to that interface.
- Global service policies provide default services to all interfaces. Unless overridden by an interface-specific policy, the global services are applied. By default, a global policy exists that includes a service policy rule for default application inspection. See Defaults for Service Policies, page 1-9 for more information. You can add a rule to the global policy using the wizard.

For information on the features you can configure with service policies, see Features Configured with Service Policies, page 1-4.

Step 1  Choose **Configuration > Firewall > Service Policy Rules**, and click Add or Add > Add Service Policy Rule.
Step 2
In the Create a Service Policy and Apply To area:

a. Choose whether the policy applies to a specific Interface or Global to all interfaces.

b. If you select Interface, choose the name of the interface. If the interface already has a policy, then you are adding a rule to the existing policy.

c. If the interface does not already have a service policy, enter the name of the new policy.

d. (Optional) Enter a description for the policy.

e. (Optional) Check the Drop and log unsupported IPv6 to IPv6 traffic option to generate a syslog (767001) for IPv6 traffic that is dropped by application inspections that do not support IPv6 traffic. By default, syslogs are not generated. For a list of inspections that support IPv6, see IPv6 Guidelines, page 1-8.

f. Click Next.

Step 3
On the Traffic Classification Criteria page, choose one of the following options to specify the traffic to which to apply the policy actions and click Next.

- Create a new traffic class. Enter a traffic class name and an optional description.

Identify the traffic using one of several criteria:

- Default Inspection Traffic—The class matches the default TCP and UDP ports used by all applications that the ASA can inspect. When you click Next, you are shown the services and ports defined by this class.

  This option, which is used in the default global policy, is a special shortcut that when used in a rule, ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For more information, see Default Class Maps (Traffic Classes), page 1-9.
See Default Inspections and NAT Limitations, page 7-5 for a list of default ports. The ASA includes a default global policy that matches the default inspection traffic, and applies common inspections to the traffic on all interfaces. Not all applications whose ports are included in the Default Inspection Traffic class are enabled by default in the policy map.

You can specify a Source and Destination IP Address class (which uses an ACL) along with the Default Inspection Traffic class to narrow the matched traffic. Because the Default Inspection Traffic class specifies the ports and protocols to match, any ports and protocols in the ACL are ignored.

- **Source and Destination IP Address (uses ACL)**—The class matches traffic specified by an extended ACL. If the ASA is operating in transparent firewall mode, you can use an EtherType ACL. When you click **Next**, you are prompted for the attributes of the access control entry. The wizard builds the ACL, you cannot select an existing ACL.
  
  When defining the ACE, the Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.

  **Note** When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying **Add rule to existing traffic class** (see below).

- **Tunnel Group**—The class matches traffic for a tunnel group (connection profile) to which you want to apply QoS. You can also specify one other traffic match option to refine the traffic match, excluding Any Traffic, Source and Destination IP Address (uses ACL), or Default Inspection Traffic.

  When you click **Next**, you are prompted to select the tunnel group (you can create a new one if necessary). To police each flow, check **Match flow destination IP address**. All traffic going to a unique IP destination address is considered a flow.

- **TCP or UDP Destination Port**—The class matches a single port or a contiguous range of ports. When you click **Next**, you are prompted to choose either TCP or UDP and enter the port number; click ... to choose one already defined in ASDM.

  **Tip** For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- **RTP Range**—The class map matches RTP traffic. When you click **Next**, you are prompted to enter an RTP port range, between 2000 and 65534. The maximum number of ports in the range is 16383.

- **IP DiffServ CodePoints (DSCP)**—The class matches up to eight DSCP values in the IP header. When you click **Next**, you are prompted to select or enter the desired values (move them into the Match on DSCP list).

- **IP Precedence**—The class map matches up to four precedence values, represented by the TOS byte in the IP header. When you click **Next**, you are prompted for the values.
Chapter 1  Service Policy

Configure Service Policies

–  Any Traffic—Matches all traffic.

• Add rule to existing traffic class. If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing ACL. You can add an ACE to any ACL that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add multiple ACEs to the same traffic class by repeating this entire procedure. See Manage the Order of Service Policy Rules, page 1-15 for information about changing the order of ACEs. When you click Next, you are prompted for the attributes of the access control entry.

• Use an existing traffic class. If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any class-map commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).

• Use class default as the traffic class. This option uses the class-default class, which matches all traffic. The class-default class is created automatically by the ASA and placed at the end of the policy. If you do not apply any actions to it, it is still created by the ASA, but for internal purposes only. You can apply actions to this class, if desired, which might be more convenient than creating a new traffic class that matches all traffic. You can only create one rule for this service policy using the class-default class, because each traffic class can only be associated with a single rule per service policy.

Step 4  If you selected a traffic matching criteria that requires additional configuration, enter the desired parameters and click Next.

Step 5  On the Rule Actions page, configure one or more rule actions. See Features Configured with Service Policies, page 1-4 for a list of features and actions that you can apply, with pointers to additional details.

Step 6  Click Finish.

Add a Service Policy Rule for Management Traffic

To add a service policy rule for traffic directed to the ASA for management purposes, use the Add Service Policy Rule wizard. You will be asked to choose the scope of the policy, for a specific interface or global:

• Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with RADIUS accounting inspection, and an interface policy with connection limits, then both RADIUS accounting and connection limits are applied to the interface. However, if you have a global policy with RADIUS accounting, and an interface policy with RADIUS accounting, then only the interface policy RADIUS accounting is applied to that interface.

• Global service policies provide default services to all interfaces. Unless overridden by an interface-specific policy, the global services are applied. By default, a global policy exists that includes a service policy rule for default application inspection. See Defaults for Service Policies, page 1-9 for more information. You can add a rule to the global policy using the wizard.

For information on the features you can configure with service policies, see Features Configured with Service Policies, page 1-4.
Configure Service Policies

Chapter 1      Service Policy

Configure Service Policies

Step 1 Choose Configuration > Firewall > Service Policy Rules, and click Add or Add > Add Management Service Policy Rule.

Step 2 In the Create a Service Policy and Apply To area:

a. Choose whether the policy applies to a specific Interface or Global to all interfaces.

b. If you select Interface, choose the name of the interface. If the interface already has a policy, then you are adding a rule to the existing policy.

c. If the interface does not already have a service policy, enter the name of the new policy.

d. (Optional) Enter a description for the policy.

e. Click Next.

Step 3 On the Traffic Classification Criteria page, choose one of the following options to specify the traffic to which to apply the policy actions and click Next.

- Create a new traffic class. Enter a traffic class name and an optional description.

  Identify the traffic using one of several criteria:

  - Source and Destination IP Address (uses ACL)—The class matches traffic specified by an extended ACL. If the ASA is operating in transparent firewall mode, you can use an EtherType ACL. When you click Next, you are prompted for the attributes of the access control entry. The wizard builds the ACL, you cannot select an existing ACL.

    When defining the ACE, the Match option creates a rule where traffic matching the addresses have actions applied. The Do Not Match option exempts the traffic from having the specified actions applied. For example, you want to match all traffic in 10.1.1.0/24 and apply connection limits to it, except for 10.1.1.25. In this case, create two rules, one for 10.1.1.0/24 using the Match option and one for 10.1.1.25 using the Do Not Match option. Be sure to arrange the rules so that the Do Not Match rule is above the Match rule, or else 10.1.1.25 will match the Match rule first.

  - TCP or UDP Destination Port—The class matches a single port or a contiguous range of ports.

    When you click Next, you are prompted to choose either TCP or UDP and enter the port number; click ... to choose one already defined in ASDM.

  Tip For applications that use multiple, non-contiguous ports, use the Source and Destination IP Address (uses ACL) to match each port.

- Add rule to existing traffic class. If you already have a service policy rule on the same interface, or you are adding to the global service policy, this option lets you add an ACE to an existing ACL. You can add an ACE to any ACL that you previously created when you chose the Source and Destination IP Address (uses ACL) option for a service policy rule on this interface. For this traffic class, you can have only one set of rule actions even if you add multiple ACEs. You can add multiple ACEs to the same traffic class by repeating this entire procedure. See Manage the Order of Service Policy Rules, page 1-15 for information about changing the order of ACEs. When you click Next, you are prompted for the attributes of the access control entry.

- Use an existing traffic class. If you created a traffic class used by a rule on a different interface, you can reuse the traffic class definition for this rule. Note that if you alter the traffic class for one rule, the change is inherited by all rules that use that traffic class. If your configuration includes any class-map commands that you entered at the CLI, those traffic class names are also available (although to view the definition of the traffic class, you need to create the rule).
Step 4 If you selected a traffic matching criteria that requires additional configuration, enter the desired parameters and click Next.

Step 5 On the Rule Actions page, configure one or more rule actions.

- To configure RADIUS accounting inspection, choose an inspect map from the RADIUS Accounting Map drop-down list, or click Configure to add a map. See Features Configured with Service Policies, page 1-4 for more information.
- To configure connection settings, see Configure Connection Settings for Specific Traffic Classes (All Services), page 12-11.

Step 6 Click Finish.

Manage the Order of Service Policy Rules

The order of service policy rules on an interface or in the global policy affects how actions are applied to traffic. See the following guidelines for how a packet matches rules in a service policy:

- A packet can match only one rule in a service policy for each feature type.
- When the packet matches a rule that includes actions for a feature type, the ASA does not attempt to match it to any subsequent rules including that feature type.
- If the packet matches a subsequent rule for a different feature type, however, then the ASA also applies the actions for the subsequent rule.

For example, if a packet matches a rule for connection limits, and also matches a rule for application inspection, then both rule actions are applied.

If a packet matches a rule for application inspection, but also matches another rule that includes application inspection, then the second rule actions are not applied.

If your rule includes an ACL with multiple ACEs, then the order of ACEs also affects the packet flow. 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. For example, if you create an ACE at the beginning of an ACL that explicitly permits all traffic, no further statements are ever checked.

To change the order of rules or ACEs within a rule, perform the following steps:

Step 1 On the Configuration > Firewall > Service Policy Rules pane, choose the rule or ACE that you want to move up or down.

Step 2 Click the Move Up or Move Down button.
Note  If you rearrange ACEs in an ACL that is used in multiple service policies, then the change is inherited in all service policies.

Step 3  When you are done rearranging your rules or ACEs, click Apply.

### 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: <code>class-map type management</code>, and <code>inspect radius-accounting</code>.</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: <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, regex, match regex</code>.</td>
</tr>
<tr>
<td>Match any for inspection policy maps</td>
<td>8.0(2)</td>
<td>The <code>match any</code> keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only <code>match all</code> was available.</td>
</tr>
</tbody>
</table>
Special Actions for Application Inspections (Inspection Policy Map)

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the service policy, you can also optionally enable actions as defined in an inspection policy map. When the inspection policy map matches traffic within the service policy for which you have defined an inspection action, then that subset of traffic will be acted upon as specified (for example, dropped or rate-limited).

- Information About Inspection Policy Maps, page 2-1
- Guidelines and Limitations, page 2-2
- Default Inspection Policy Maps, page 2-2
- Defining Actions in an Inspection Policy Map, page 2-3
- Identifying Traffic in an Inspection Class Map, page 2-3
- Where to Go Next, page 2-4
- Feature History for Inspection Policy Maps, page 2-4

Information About Inspection Policy Maps

See Configure Application Layer Protocol Inspection, page 7-8 for a list of applications that support inspection policy maps.

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 option—You can define a traffic matching option directly in the inspection policy map to match application traffic to criteria specific to the application, such as a URL string, for which you then enable actions.
  - Some traffic matching options can specify 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—An inspection class map includes multiple traffic matching options. You then identify the class map in the policy map and enable actions for the class map 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. Note: Not all inspections support inspection class maps.
Guidelines and Limitations

- Parameters—Parameters affect the behavior of the inspection engine.

Default Inspection Policy Maps

DNS inspection is enabled by default, using the preset_dns_map inspection class map:

- The maximum DNS message length is 512 bytes.
- 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.
Defining Actions in a Policy Map

When you enable an inspection engine in the service policy, you can also optionally enable actions as defined in an inspection policy map.

**Detailed Steps**

**Step 1** (Optional) Create an inspection class map. Alternatively, you can identify the traffic directly within the policy map. See Identifying Traffic in an Inspection Class Map, page 2-3.

**Step 2** (Optional) For policy map types that support regular expressions, create a regular expression. See the general operations configuration guide.

**Step 3** Choose Configuration > Firewall > Objects > Inspect Maps.

**Step 4** Choose the inspection type you want to configure.

**Step 5** Click Add to add a new inspection policy map.

**Step 6** Follow the instructions for your inspection type in the inspection chapter.

Identifying Traffic in an Inspection Class Map

This type of class map allows you to match criteria that is specific to an application. For example, for DNS traffic, you can match the domain name in a DNS query.

A class map groups multiple traffic matches (in a match-all class map), or lets you match any of a list of matches (in a match-any class 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 group multiple match commands, and you can reuse class maps. For the traffic that you identify in this class map, you can specify actions such as dropping, resetting, and/or logging the connection in the inspection policy map. If you want to perform different actions on different types of traffic, you should identify the traffic directly in the policy map.

**Restrictions**

Not all applications support inspection class maps.

**Detailed Steps**

**Step 1** Choose Configuration > Firewall > Objects > Class Maps.

**Step 2** Choose the inspection type you want to configure.

**Step 3** Click Add to add a new inspection class map.
Step 4  Follow the instructions for your inspection type in the inspection chapter.

Where to Go Next

To use an inspection policy, see Chapter 1, “Service Policy.”

Feature History for Inspection Policy Maps

Table 2-1 lists the release history for this feature.

Table 2-1  Feature History for Service Policies

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</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: 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>Match any for inspection policy maps</td>
<td>8.0(2)</td>
<td>The match any keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only match all was available.</td>
</tr>
</tbody>
</table>
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, page 3-1
- Guidelines for Access Control, page 3-6
- Configure Access Control, page 3-7
- Monitoring Access Rules, page 3-13
- History for Access Rules, page 3-14

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 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 (transparent firewall mode 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.

In transparent firewall mode, you can combine extended access rules, management access rules, and EtherType rules on the same interface.

- General Information About Rules, page 3-2
General Information About Rules

This section describes information for both access rules and EtherType rules, and it includes the following topics:

- Interface Access Rules and Global Access Rules, page 3-2
- Inbound and Outbound Rules, page 3-2
- Rule Order, page 3-3
- Implicit Permits, page 3-3
- Implicit Deny, page 3-4
- NAT and Access Rules, page 3-4

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.
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

For routed mode, the following types of traffic are allowed through by default:
- Unicast IPv4 and IPv6 traffic from a higher security interface to a lower security interface.

For transparent mode, the following types of traffic are allowed through by default:
- Unicast IPv4 and IPv6 traffic from a higher security interface to a lower security interface.
- ARPs in both directions. (You can control ARP traffic using ARP inspection, but you cannot control it by access rule.)
- BPDUs in both directions.

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 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. Global access rule.
3. 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, page 3-4
- Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules, page 3-5
- Management Access Rules, page 3-5

Extended Access Rules for Returning Traffic

For TCP and UDP 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.
Chapter 3 Access Rules

Controlling Network Access

Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules

In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Transparent firewall mode can allow any IP traffic through.

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

The following table lists common traffic types that you can allow through the transparent firewall.

<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 (such as HTTP, Telnet, and SSH connections to an interface) have higher precedence than a management access rule. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box ACL.

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, page 3-5
- EtherType Rules for Returning Traffic, page 3-6
- Allowing MPLS, page 3-6

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 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.

```
hostname(config)# mpls ldp router-id interface force
```

Or

```
hostname(config)# tag-switching tdp router-id interface force
```

**Guidelines for Access Control**

**IPv6 Guidelines**

Supports IPv6. (9.0 and later) The source and destination addresses can include any mix of IPv4 and IPv6 addresses. For pre-9.0 versions, you must create a separate IPv6 access rule.

**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 rule of lookup performance. When enabled, object group search does not expand network objects, but instead searches access rules for matches based on those group definitions. You can set this option by clicking the **Advanced** button below the access rule table.
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. The option is under Configurations > Device Management > Advanced > Rule Engine.

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, select the option in the access rules advanced settings; choose Configuration > Access Rules and click the Advanced button.

Configure Access Control

The following topics explain how to configure access control.

- Configure Access Rules, page 3-7
- Configure Management Access Rules, page 3-11
- Configure EtherType Rules (Transparent Mode Only), page 3-11
- Configure ICMP Access Rules, page 3-12

Configure Access Rules

To apply an access rule, perform the following steps.

Procedure

**Step 1** Choose Configuration > Firewall > Access Rules.

The rules are organized by interface and direction, with a separate group for global rules. If you configure management access rules, they are repeated on this page. These groups are equivalent to the extended ACL that is created and assigned to the interface or globally as an access group. These ACLs also appear on the ACL Manager page.

**Step 2** Do any of the following:

- To add a new rule, choose Add > Add Access Rule.
- To insert a rule at a specific location within a container, select an existing rule and choose Add > Insert to add the rule above it, or choose Add > Insert After.
- To edit a rule, select it and click Edit.

**Step 3** Fill in the rule properties. The primary options to select are:

- **Interface**—The interface to which the rule applies. Select Any to create a global rule.
- **Action: Permit/Deny**—Whether you are permitting (allowing) the described traffic or are denying (dropping) it.
Configure Access Control

Chapter 3      Access Rules

Step 4  Click **Apply** to save the access rule to your configuration.

**Access Rule Properties**

When you add or edit an access rule, you can configure the following properties. In many fields, you can click the “...” button on the right of the edit box to select, create, or edit objects that are available for the field.

- **Interface**—The interface to which the rule applies. Select Any to create a global rule.
- **Action: Permit/Deny**—Whether you are permitting (allowing) the described traffic or are denying (dropping) it.
- **Source Criteria**—The characteristics of the originator of the traffic you are trying to match. You must configure Source, but the other properties are optional.
  - **Source**—The IPv4 or IPv6 address of the source. The default is *any*, which matches all IPv4 or IPv6 addresses; you can use *any4* to target IPv4 only, or *any6* to target IPv6 only. You can specify a single host address (such as 10.100.10.5 or 2001:DB8::0DB8:800:200C:417A), a subnet (in 10.100.10.0/24 or 10.100.10.0/255.255.255.0 format, or for IPv6, 2001:DB8:0:CD30::/60), the name of a network object or network object group, or the name of an interface.
  - **User**—If you enable the identity firewall, you can specify a user or user group as the traffic source. The IP address the user is currently using will match the rule. You can specify a username (DOMAIN\user), a user group (DOMAIN\group, note the double \ indicates a group name), or a user object group. For this field, it is far easier to click “...” to select names from your AAA server group than to type them in.
  - **Security Group**—If you enable Cisco Trustsec, you can specify a security group name or tag (1-65533), or security group object.
  - **More Options > Source Service**—If you specify TCP or UDP as the destination service, you can optionally specify a predefined service object for TCP, UDP, or TCP-UDP, or use your own object. Typically, you define the destination service only and not the source service. Note that if you define the source service, the destination service protocol must match it (for example, both TCP, with or without port definitions).
- **Destination Criteria**—The characteristics of the target of the traffic you are trying to match. You must configure Destination, but the other properties are optional.
  - **Destination**—The IPv4 or IPv6 address of the destination. The default is *any*, which matches all IPv4 or IPv6 addresses; you can use *any4* to target IPv4 only, or *any6* to target IPv6 only. You can specify a single host address (such as 10.100.10.5 or 2001:DB8::0DB8:800:200C:417A), a subnet (in 10.100.10.0/24 or 10.100.10.0/255.255.255.0 format, or for IPv6, 2001:DB8:0:CD30::/60), the name of a network object or network object group, or the name of an interface.

For detailed information on all of the available options, see **Access Rule Properties**, page 3-8.
- **Security Group**—If you enable Cisco Trustsec, you can specify a security group name or tag (1-65533), or security group object.

- **Service**—The protocol of the traffic, such as IP, TCP, UDP, and optionally ports for TCP and UDP. The default is IP, but you can select a more specific protocol to target traffic with more granularity. Typically, you would select some type of service object. For TCP and UDP, you can specify ports, for example, tcp/80, tcp/http, tcp/10-20 (for a range of ports), tcp-udp/80 (match any TCP or UDP traffic on port 80), and so forth.

- **Description**—A explanation of the purpose of the rule, up to 100 characters per line. You can enter multiple lines; each line is added as a remark in the CLI, and the remarks are placed before the rule.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you add remarks with non-English characters on one platform (such as Windows) then try to remove them from another platform (such as Linux), you might not be able to edit or delete them because the original characters might not be correctly recognized. This limitation is due to an underlying platform dependency that encodes different language characters in different ways.</td>
</tr>
</tbody>
</table>

- **Enable Logging: Logging Level: More Options > Logging Interval**—The logging options define how syslog messages will be generated for rules. You can implement the following logging options:

  - **Deselect Enable Logging**—This will disable logging for the rule. No syslog messages of any type will be issued for traffic that matches this rule.

  - **Select Enable Logging with Logging Level = Default**—This provides the default logging for rules. Syslog message 106023 is issued for each denied packet. If the appliance comes under attack, the frequency of issuing this message could impact services.

  - **Select Enable Logging with Non-Default Logging Level**—This provides a summarized syslog message, 106100, instead of 106023. Message 106100 is issued upon first hit, then again at each interval configured in More Options > Logging Interval (default is every 300 seconds, you can specify 1-600), showing the number of hits during that interval. The recommended logging level is **Informational**.

  Summarizing deny messages can reduce the impact of attacks and possibly make it easier for you to analyze messages. If you do come under a denial of service attack, you might see message 106101, which indicates that the number of cached deny flows used to produce the hit count for message 106100 has exceeded the maximum for an interval. At this point, the appliance stops collecting statistics until the next interval to mitigate the attack.

- **More Options > Traffic Direction**—Whether the rule is for the **In** or **Out** direction. **In** is the default, and it is the only option for global and management access rules.

- **More Options > Enable Rule**—Whether the rule is active on the device. Disabled rules appear with strike-through text in the rule table. Disabling a rule lets you stop its application to traffic without deleting it, so you can enable it again later if you decide you need it.

- **More Options > Time Range**—The name of the time range object that defines the times of day and days of the week when the rule should be active. If you do not specify a time range, the rule is always active.

### Configuring Advanced Options for Access Rules

Advanced access rule options allow you to customize certain aspects of rule behavior, but these options have defaults that are appropriate in most cases.
### Configure Access Control

**Step 1** Choose **Configuration > Firewall > Access Rules**.

**Step 2** Click the **Advanced** button below the rule table.

**Step 3** Configure the following options as required:

- **Advanced Logging Settings**—If you configure non-default logging, the system caches deny flows to develop statistics for message 106100, as explained in Evaluating Syslog Messages for Access Rules, page 3-13. To prevent unlimited consumption of memory and CPU resources, the ASA places a limit on the number of concurrent *deny* flows because they can indicate an attack. Message 106101 is issued when the limit is reached. You can control the following aspects related to 106101.
  - Maximum Deny-flows—The maximum number of deny flows permitted before the ASA stops caching flows, between 1 and 4096. The default is 4096.
  - Alert Interval—The amount of time (1-3600 seconds) between issuing system log message 106101, which indicates that the maximum number of deny flows was reached. The default is 300 seconds.

- **Per User Override table**—Whether to allow a dynamic user ACL that is downloaded for user authorization from a RADIUS server 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. Check the **Per User Override** box for each interface that should allow user overrides (inbound direction only). If the per user override feature is disabled, the access rule provided by the RADIUS server is combined with the access rule configured on that interface.

By default, VPN remote access traffic is not matched against interface ACLs. However, if you deselect the **Enable inbound VPN sessions to bypass interface access lists** setting on the Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles pane, the behavior depends on whether there is a VPN filter applied in the group policy (see the Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter field) 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.

- **Object Group Search Setting**—You can reduce the memory required to search access rules that use object groups by selecting **Enable Object Group Search Algorithm**, but this is at the expense of rule lookup performance. When enabled, object group search does not expand network objects, but instead searches access rules for matches based on those group definitions.

- **Forward Reference Setting**—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. Select **Enable the forward reference of objects and object-groups** to enable forward referencing. Be aware that if you enable forward referencing, ASDM cannot tell the difference between a typo reference to an existing object and a forward reference.

**Step 4** Click **OK**.
Configure Management Access Rules

You can configure an interface ACL that controls to-the-box management traffic from a specific peer (or set of peers) to the ASA. One scenario in which this type of ACL would be useful is when you want to block IKE Denial of Service attacks.

To configure an extended ACL that permits or denies packets for to-the-box traffic, perform the following steps.

**Step 1** Choose Configuration > Device Management > Management Access > Management Access Rules.

The rules are organized by interface. Each group is equivalent to the extended ACL that is created and assigned to the interface as a control plane ACL. These ACLs also appear on the Access Rules and ACL Manager pages.

**Step 2** Do any of the following:

- To add a new rule, choose Add > Add Management Access Rule.
- To insert a rule at a specific location within a container, select an existing rule and choose Add > Insert to add the rule above it, or choose Add > Insert After.
- To edit a rule, select it and click Edit.

**Step 3** Fill in the rule properties. The primary options to select are:

- **Interface**—The interface to which the rule applies.
- **Action: Permit/Deny**—Whether you are permitting (allowing) the described traffic or are denying (dropping) it.
- **Source/Destination criteria**—A definition of the source (originating address) and destination (target address of the traffic flow). You typically configure IPv4 or IPv6 addresses of hosts or subnets, which you can represent with network or network object groups. You can also specify a user or user group name for the source. Additionally, you can use the Service field to identify the specific type of traffic if you want to focus the rule more narrowly than all IP traffic. If you implement Trustsec, you can use security groups to define source and destination.

For detailed information on all of the available options, see Access Rule Properties, page 3-8.

When you are finished defining the rule, click OK to add the rule to the table.

**Step 4** Click Apply to save the rule to your configuration.

Configure EtherType Rules (Transparent Mode Only)

EtherType rules apply to non-IP layer-2 traffic in transparent firewall mode. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet. With EtherType rules, you can control the flow of non-IP traffic across the ASA.

In transparent mode, you can apply both extended and EtherType access rules to an interface. EtherType rules take precedence over the extended access rules.

To add an EtherType rule, perform the following steps.
**Step 1** Choose **Configuration > Firewall > EtherType Rules**.

The rules are organized by interface and direction. Each group is equivalent to the EtherType ACL that is created and assigned to the interface.

**Step 2** Do any of the following:

- To add a new rule, choose **Add > Add EtherType Rule**.
- To insert a rule at a specific location within a container, select an existing rule and choose **Add > Insert** to add the rule above it, or choose **Add > Insert After**.
- To edit a rule, select it and click **Edit**.

**Step 3** Fill in the rule properties. The primary options to select are:

- **Interface**—The interface to which the rule applies.
- **Action: Permit/Deny**—Whether you are permitting (allowing) the described traffic or are denying (dropping) it.
- **EtherType**—You can match traffic using the following options:
  - **ipx**—Internet Packet Exchange (IPX).
  - **bpdu**—bridge protocol data units, which are allowed by default.
  - **mpls-multicast**—MPLS multicast.
  - **mpls-unicast**—MPLS unicast.
  - **isis**—Intermediate System to Intermediate System (IS-IS).
  - **any**—Matches all traffic.
  - **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.
- **Description**—A explanation of the purpose of the rule, up to 100 characters per line. You can enter multiple lines; each line is added as a remark in the CLI, and the remarks are placed before the rule.
- **More Options > Direction**—Whether the rule is for the **In** or **Out** direction. **In** is the default.

When you are finished defining the rule, click **OK** to add the rule to the table.

**Step 4** Click **Apply** to save the rule to your configuration.

---

**Configure ICMP Access Rules**

By default, you can send ICMP packets to any ASA 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 ASA 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. See RFC 1195 and RFC 1435 for details about path MTU discovery.

Procedure

Step 1 Choose Configuration > Device Management > Management Access > ICMP.

Step 2 Configure ICMP rules:

a. Add a rule (Add > Rule, Add > IPv6 Rule, or Add > Insert), or select a rule and edit it.

b. Select the ICMP type you want to control, or any to apply to all types.

c. Select the interface to which the rule applies. You must create separate rules for each interface.

d. Select whether you are permitting or denying access for matching traffic.

e. Select Any Address to apply the rule to all traffic. Alternatively, enter the address and mask (for IPv4) or address and prefix length (for IPv6) of the host or network you are trying to control.

f. Click OK.

Step 3 (Optional) To set ICMP unreachable message limits, set the following options. Increasing the rate limit, along with enabling the Decrement time to live for a connection option in a service policy (on the Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings dialog box), is required to allow a trace route through the ASA that shows the ASA as one of the hops.

- Rate Limit—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
- Burst Size—Sets the burst rate, between 1 and 10. This keyword is not currently used by the system, so you can choose any value.

Step 4 Click Apply.

Monitoring Access Rules

The Access Rules page includes hit counts for each rule. Mouse over the hit count to see the update time and interval for the count. To reset the hit count, right click the rule and select Clear Hit Count, but be aware that this clears the count for all rules applied to the same interface in the same direction.

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, and the maximum number of deny flows cached, in the advanced settings; see Configuring Advanced Options for Access Rules, page 3-9.

## 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 screen: Configuration &gt; Firewall &gt; Access Rules.</td>
</tr>
<tr>
<td>Global access rules</td>
<td>8.3(1)</td>
<td>Global access rules were introduced. We modified the following screen: Configuration &gt; Firewall &gt; Access Rules.</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.</td>
</tr>
</tbody>
</table>
EtherType ACL support for IS-IS traffic

8.4(5), 9.1(2)

In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL.

We modified the following screen: Configuration > Device Management > Management Access > EtherType Rules.

Support for TrustSec

9.0(1)

You can now use TrustSec security groups for the source and destination. You can use an identity firewall ACL with access rules.

Unified ACL for IPv4 and IPv6

9.0(1)

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 screens:
Configuration > Firewall > Access Rules
Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options

Extended ACL and object enhancement to filter ICMP traffic by ICMP code

9.0(1)

ICMP traffic can now be permitted/denied based on ICMP code.

We introduced or modified the following screens:
Configuration > Firewall > Objects > Service Objects/Groups
Configuration > Firewall > Access Rule

Transactional Commit Model on Access Group Rule Engine

9.1(5)

When enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance.

We introduced the following screen: Configuration > Device Management > Advanced > Rule Engine.

Configuration session for editing ACLs and objects.
Forward referencing of objects and ACLs in access rules.

9.3(2)

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.
Public Servers

The following topics describe how to configure public servers.

- Expose a Server to the Public, page 4-1
- History for Public Servers, page 4-2

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.

ASDM includes a short cut for configuring the required access and NAT rules, to simplify the process of exposing a service on an internal server to the public.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Firewall &gt; Public Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Click Add.</td>
</tr>
<tr>
<td></td>
<td>• Select an existing public server and click Edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Define the private and public characteristics of the service you are exposing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private Interface</strong>—The interface to which the real server is connected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private IP Address</strong>—The host network object that defines the real IPv4 address of the server. You cannot specify an IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private Service</strong>—The actual service that is running on the real server. You can use a pre-defined service or service object. You can also use a service object group unless you also specify a public service to which you are mapping the private service.</td>
</tr>
</tbody>
</table>
You can expose multiple services; however, if you specify a public service, all ports are mapped to the same public port.

- **Public Interface**—The interface through which outside users can access the real server.
- **Public Address**—The IPv4 address that is seen by outside users. You can specify the address directly or use a host network object.
- **Specify Public Service if different from private service.** **Public Service**—The service that is running on the translated address. Specify the public service only if it differs from the private service. For example, if the private web server runs on TCP/80, and you want to use the same port for external users, there is no need to specify the public service. You must use a pre-defined TCP or UDP service if you specify a public service.

**Step 4** Click **OK**, then click **Apply**.

---

**Related Topics**
- **About Static NAT, page 5-38**

---

**History for Public Servers**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Servers</td>
<td>8.3(1)</td>
<td>Public servers provide internal and external users access to various application servers. We introduced the following screen: Configuration &gt; Firewall &gt; Public Servers</td>
</tr>
</tbody>
</table>
PART 2

Network Address Translation
Network Address Translation (NAT)

The following topics explain Network Address Translation (NAT) and how to configure it.

- Why Use NAT?, page 5-1
- NAT Basics, page 5-2
- Guidelines for NAT, page 5-6
- Dynamic NAT, page 5-11
- Dynamic PAT, page 5-20
- Static NAT, page 5-38
- Identity NAT, page 5-50
- Monitoring NAT, page 5-57
- History for NAT, page 5-57

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.
NAT Basics

The following topics explain some of the basics of NAT.

- NAT Terminology, page 5-2
- NAT Types, page 5-3
- Network Object NAT and Twice NAT, page 5-3
- NAT Rule Order, page 5-5
- NAT Interfaces, page 5-6

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 ASA, 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 residing on the ASA’s 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.

- 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) (Version 9.0(1) and later)—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 Types

You can implement NAT using the following methods:

- Dynamic NAT—A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses, on a first come, first served basis. Only the real host can initiate traffic. See Dynamic NAT, page 5-11.

- 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, page 5-20.

- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See Static NAT, page 5-38.

- 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, page 5-50.

Network Object NAT and Twice NAT

The ASA 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. Network object NAT is easier to configure, and might be more reliable for applications such as Voice over IP (VoIP). (For VoIP, because twice NAT is applicable only between two objects, you might see a failure in the translation of indirect addresses that do not belong to either of the objects.)

- Network Object NAT, page 5-3
- Twice NAT, page 5-3
- Comparing Network Object NAT and Twice NAT, page 5-4

Network Object NAT

All NAT rules that are configured as a parameter of a network object are considered to be network object NAT rules. Network object NAT is a quick and easy way to configure NAT for a network object, which can be a single IP address, a range of addresses, or a subnet.

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 the ASA, 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 (twice NAT lets you 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.
Note

For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address. For example, if you configure static NAT with port address translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then in the command, 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.

Twice NAT also lets you use service objects for static NAT with port translation; network object NAT only accepts inline definition.

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 matching packet only matches the one rule, and further rules are not checked. Even if you do not configure the optional destination address for twice NAT, a matching packet still only matches one twice NAT rule. 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 rules 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 5-1  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. Note If you configure EasyVPN remote, the ASA dynamically adds invisible NAT rules to the end of this section. Be sure that you do not configure a twice NAT rule in this section that might match your VPN traffic, instead of matching the invisible rule. If VPN does not work due to NAT failure, consider adding twice NAT rules to section 3 instead.</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, as automatically determined by the ASA: 1. Static rules. 2. Dynamic rules. Within each rule type, the following ordering guidelines are used: 1. Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. 2. For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. 3. If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.</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. You can specify whether to add a twice NAT rule to section 3 when you add the rule.</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)
Guidelines for NAT

The following topics provide detailed guidelines for implementing NAT.

- Firewall Mode Guidelines for NAT, page 5-7
- IPv6 NAT Guidelines, page 5-7

NAT Interfaces

In routed mode, 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 5-1 Specifying Any Interface

In transparent mode, you must choose specific source and destination interfaces.

Guidelines for NAT
Firewall Mode Guidelines for NAT

NAT is supported in routed and transparent firewall mode. However, transparent mode has the following restrictions:

- In transparent mode, you must specify the real and mapped interfaces; you cannot specify “any” as the interface.
- In transparent mode, you cannot configure interface PAT, because the transparent mode interfaces do not have IP addresses. You also cannot use the management IP address as a mapped address.
- In transparent mode, translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

IPv6 NAT Guidelines

NAT supports IPv6 with the following guidelines and restrictions.

- For routed mode, you can also translate between IPv4 and IPv6.
- For transparent mode, translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.
- For transparent mode, a PAT pool is not supported for IPv6.
- 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 192.168.1.4 will...
be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address. You can also optionally translate the addresses net-to-net, where the first IPv4 address maps to the first IPv6 address, the second to the second, and so on.

- **NAT64 (IPv6-to-IPv4)**—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

### Additional Guidelines for NAT

- **(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.

- **(Twice NAT only.)** You cannot configure FTP destination port translation when the source IP address is a subnet (or any other application that uses a secondary connection); the FTP data channel establishment does not succeed.

- 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. 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.

- 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 the `any` keyword 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), use the interface name instead of the IP address.
  - (Transparent mode) The management IP address.
  - (Dynamic NAT) The standby interface IP address when VPN is enabled.
  - Existing VPN pool addresses.
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.

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, page 5-8 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.
Guidelines for NAT

- 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.

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, page 5-8 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, page 5-4.

- 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**

Consider the following guidelines when creating objects for twice NAT:

- NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP).
- 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, page 5-12**
- **Configure Dynamic Network Object NAT, page 5-14**
- **Configure Dynamic Twice NAT, page 5-15**
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, the ASA assigns the host an IP address from the mapped pool. The translation is created only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, even if the connection is allowed by an access rule.

Note

For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

The following figure shows a typical dynamic NAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back.

Figure 5-2 Dynamic NAT
The following figure shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the ASA drops the packet.

**Figure 5-3 Remote Host Attempts to Initiate a Connection to a Mapped Address**

![Diagram showing the attempt of a remote host to initiate a connection to a mapped address]

**Dynamic NAT Disadvantages and Advantages**

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.
  
  Use PAT or a PAT fall-back method if this event occurs often because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool, and routable addresses may not be available in large quantities.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.

- Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

See Default Inspections and NAT Limitations, page 7-5 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  Add NAT to a new or existing network object:
- To add a new network object, choose **Configuration > Firewall > NAT Rules**, then click **Add > Add Network Object NAT Rule**.
- To add NAT to an existing network object, choose **Configuration > Firewall > Objects > Network Objects/Groups**, and then edit a network object.

Step 2  For a new object, enter values for the following fields:
- **Name**—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.
- **Type**—Host, Network, or Range.
- **IP Addresses**—IPv4 or IPv6 addresses, a single address for a host, a starting and ending address for a range, and for subnet, either an IPv4 network address and mask (for example, 10.100.10.0 255.255.255.0) or IPv6 address and prefix length (for example, 2001:DB8:0:CD30::/60).

Step 3  If the NAT section is hidden, click **NAT** to expand the section.
Step 4  Check the **Add Automatic Translation Rules** check box.

Step 5  From the Type drop-down list, choose **Dynamic**.

Step 6  To the right of the Translated Addr field, click the browse button and choose the network object or network object group that contains the mapped addresses.

You can create a new object if necessary.

The object or group cannot contain a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

Step 7  (Optional, Routed Mode Only) To use the interface IP address as a backup method when the other mapped addresses are already allocated, check the **Fall through to interface PAT (dest intf)** check box, and choose the interface from the drop-down list. To use the IPv6 address of the interface, also check the **Use IPv6 for interface PAT** check box.

Step 8  (Optional) Click **Advanced**, configure the following options in the Advanced NAT Settings dialog box, and click **OK**.

- **Translate DNS replies for rule**—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See DNS and NAT, page 6-39 for more information.

- (Required for Transparent Firewall Mode.) **Interface**—Specifies the real interface (**Source**) and the mapped interface (**Destination**) where this NAT rule applies. By default, the rule applies to all interfaces.

Step 9  Click **OK**, and then **Apply**.

---

**Configure Dynamic Twice NAT**

This section describes how to configure twice NAT for dynamic NAT.

**Procedure**

Step 1  Choose **Configuration > Firewall > NAT Rules**, and then do one of the following:

- Click **Add**, or **Add > Add NAT Rule Before Network Object NAT Rules**.
- Click **Add > Add NAT Rule After Network Object NAT Rules**.
- Select a twice NAT rule and click **Edit**.

The Add NAT Rule dialog box appears.
Step 2  Set the source and destination interfaces.
By default in routed mode, both interfaces are set to --Any--. In transparent firewall mode, you must set specific interfaces.

a. From the Match Criteria: Original Packet > Source Interface drop-down list, choose the source interface.

b. From the Match Criteria: Original Packet > Destination Interface drop-down list, choose the destination interface.

Step 3  Choose Dynamic from the Action: Translated Packet > Source NAT Type drop-down list.
This setting only applies to the source address; the destination translation is always static.
Step 4 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the source interface network (the *real source address* and the *mapped destination address*). See the following figure for an example of the original packet vs. the translated packet.

![Diagram of Original and Translated Packets]

a. For the **Match Criteria: Original Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Source Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. The default is *any*.

b. (Optional.) For the **Match Criteria: Original Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Destination Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

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, page 5-4.

Step 5 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network (the *mapped source address* and the *real destination address*). You can translate between IPv4 and IPv6 if desired.

a. For **Action: Translated Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Translated Source Address dialog box.

   For dynamic NAT, you typically configure a larger group of source addresses to be mapped to a smaller group.

   **Note** The object or group cannot contain a subnet.

b. For **Action: Translated Packet > Destination Address**, click the browse button and choose an existing network object, group, or interface or create a new object or group from the Browse Translated Destination Address dialog box.

   For identity NAT for the destination address, simply use the same object or group for both the real and mapped addresses.

   If you want to translate the destination address, then 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, page 5-38. See Additional Guidelines for NAT, page 5-8 for information about disallowed mapped IP addresses.
For static interface NAT with port translation only, choose an interface from the Browse dialog box. Be sure to also configure a service translation. For this option, you must configure a specific interface for the Source Interface. See Static Interface NAT with Port Translation, page 5-40 for more information.

**Step 6** (Optional.) Identify the destination service ports for service translation.

- Identify the original packet port (the mapped destination port). For **Match Criteria: Original Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Original Service dialog box.

- Identify the translated packet port (the real destination port). For **Action: Translated Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Translated Service dialog box.

Dynamic NAT does not support port translation. However, because the destination translation is always static, you can perform port translation for the destination port. 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. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports. The “not equal” (!=) operator is not supported.

For example:
Step 7  (Optional, Routed Mode Only.) To use the interface IP address as a backup method if the other mapped source addresses are already allocated, check the Fall through to interface PAT check box. To use the IPv6 interface address, also check the Use IPv6 for interface PAT check box.

The destination interface IP address is used. This option is only available if you configure a specific Destination Interface.

Step 8  (Optional.) Configure NAT options in the Options area.
Dynamic PAT

The following topics describe dynamic PAT.

- About Dynamic PAT, page 5-20
- Configure Dynamic Network Object PAT (Hide), page 5-22
- Configure Dynamic Network Object PAT Using a PAT Pool, page 5-24
- Configure Dynamic Twice PAT (Hide), page 5-27
- Configure Dynamic Twice PAT Using a PAT Pool, page 5-31
- Configure Per-Session PAT or Multi-Session PAT (Version 9.0(1) and Higher), page 5-36

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 5-4 Dynamic PAT**

![Diagram of Dynamic PAT](image)

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 (9.0(1) and later), the xlate is immediately removed. Users on the destination network cannot reliably initiate a connection to a host that uses PAT (even if the connection is allowed by an access rule).

**Note**

For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the 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.

**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.

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, page 7-5 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. (8.4(2)/8.5(1) and later) 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. (8.4(3) and later, not including 8.5(1) or 8.6(1)) 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 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, page 7-5 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. **Note:** This “stickiness” does not survive a failover. If the ASA fails over, then subsequent connections from a host may not use the initial IP address.

• 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 (Hide)

This section describes how to configure network object NAT for dynamic PAT (hide), which uses a single address for translation instead of a PAT pool.

**Procedure**

**Step 1** Add NAT to a new or existing network object:

• To add a new network object, choose Configuration > Firewall > NAT Rules, then click Add > Add Network Object NAT Rule.

• To add NAT to an existing network object, choose Configuration > Firewall > Objects > Network Objects/Groups, and then edit a network object.

**Step 2** For a new object, enter values for the following fields:

a. **Name**—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. **Type**—Host, Network, or Range.

c. **IP Addresses**—IPv4 or IPv6 addresses, a single address for a host, a starting and ending address for a range, and for subnet, either an IPv4 network address and mask (for example, 10.100.10.0 255.255.255.0) or IPv6 address and prefix length (for example, 2001:DB8:0:CD30:/60).

**Step 3** If the NAT section is hidden, click **NAT** to expand the section.

**Step 4** Check the **Add Automatic Translation Rules** check box.
Step 5  From the Type drop-down list, choose **Dynamic PAT (Hide)**.

![Add Network Object](image1)

Step 6  Specify a single mapped address. In the Translated Addr. field, specify the mapped IP address by doing one of the following:

- Type a host IP address.
- Click the browse button and select a host network object (or create a new one).
- (Routed mode only.) Type an interface name or click the browse button, and choose an interface from the Browse Translated Addr dialog box.

![Interfaces](image2)

If you specify an interface name, then you enable **interface PAT**, where the specified interface IP address is used as the mapped address. To use the IPv6 interface address, you must also check the **Use IPv6 for interface PAT** check box. With interface PAT, the NAT rule only applies to the specified mapped interface. (If you do not use interface PAT, then the rule applies to all interfaces by default.) You cannot specify an interface in transparent mode.

Step 7  (Optional) Click **Advanced**, configure the following options in the Advanced NAT Settings dialog box, and click **OK**.

- **Translate DNS replies for rule**—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See **DNS and NAT, page 6-39** for more information.
Dynamic PAT

- (Required for Transparent Firewall Mode.) **Interface**—Specifies the real interface (**Source**) and the mapped interface (**Destination**) where this NAT rule applies. By default, the rule applies to all interfaces.

**Step 8** Click **OK**, and then **Apply**.

---

**Configure Dynamic Network Object PAT Using a PAT Pool**

This section describes how to configure network object NAT for dynamic PAT using a PAT pool.

**Procedure**

**Step 1** Add NAT to a new or existing network object:

- To add a new network object, choose **Configuration** > **Firewall** > **NAT Rules**, then click **Add** > **Add Network Object NAT Rule**.
- To add NAT to an existing network object, choose **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**, and then edit a network object.

**Step 2** For a new object, enter values for the following fields:

a. **Name**—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. **Type**—Host, Network, or Range.

c. **IP Addresses**—IPv4 or IPv6 addresses, a single address for a host, a starting and ending address for a range, and for subnet, either an IPv4 network address and mask (for example, 10.100.10.0 255.255.255.0) or IPv6 address and prefix length (for example, 2001:DB8:0:CD30::/60).

**Step 3** If the NAT section is hidden, click **NAT** to expand the section.
Step 4 Check the **Add Automatic Translation Rules** check box.

Step 5 From the **Type** drop-down list, choose **Dynamic** even though you are configuring dynamic PAT with a PAT pool.

Step 6 To configure the PAT pool:

a. Do not enter a value for the **Translated Addr.** field; leave it blank.

b. Check the **PAT Pool Translated Address** check box, then click the browse button and choose the network object or group that contains the PAT pool addresses. or create a new object from the Browse Translated PAT Pool Address dialog box.

**Note** The PAT pool object or group cannot contain a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
e. (Optional) Check the Round Robin check box to assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

d. (Optional, 8.4(3) and later, not including 8.5(1) or 8.6(1).) Check the Extend PAT uniqueness to per destination instead of per interface check box to use extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

e. (Optional, 8.4(3) and later, not including 8.5(1) or 8.6(1).) Check the Translate TCP or UDP ports into flat range (1024-65535) check box to use the 1024 to 65535 port range as a single flat 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 check the Include range 1 to 1023 check box.

Step 7 (Optional, Routed Mode Only) To use the interface IP address as a backup method when the other mapped addresses are already allocated, check the Fall through to interface PAT (dest intf) check box, and choose the interface from the drop-down list. To use the IPv6 address of the interface, also check the Use IPv6 for interface PAT check box.

Step 8 (Optional) Click Advanced, configure the following options in the Advanced NAT Settings dialog box, and click OK.

- Translate DNS replies for rule—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See DNS and NAT, page 6-39 for more information.

- (Required for Transparent Firewall Mode.) Interface—Specifies the real interface (Source) and the mapped interface (Destination) where this NAT rule applies. By default, the rule applies to all interfaces.

Step 9 Click OK, and then Apply.
Configure Dynamic Twice PAT (Hide)

This section describes how to configure twice NAT for dynamic PAT (hide), which uses a single address for translation instead of a PAT pool.

Procedure

**Step 1** Choose Configuration > Firewall > NAT Rules, and then do one of the following:
- Click Add, or Add > Add NAT Rule Before Network Object NAT Rules.
- Click Add > Add NAT Rule After Network Object NAT Rules.
- Select a twice NAT rule and click Edit.

The Add NAT Rule dialog box appears.

**Step 2** Set the source and destination interfaces.

By default in routed mode, both interfaces are set to --Any--. In transparent firewall mode, you must set specific interfaces.

a. From the Match Criteria: Original Packet > Source Interface drop-down list, choose the source interface.
b. From the **Match Criteria: Original Packet > Destination Interface** drop-down list, choose the destination interface.

**Step 3**

Choose **Dynamic PAT (Hide)** from the **Action: Translated Packet > Source NAT Type** drop-down list. This setting only applies to the source address; the destination translation is always static.

**Note**

To configure dynamic PAT using a PAT pool, choose **Dynamic** instead of Dynamic PAT (Hide), see Configure Dynamic Twice PAT Using a PAT Pool, page 5-31.

**Step 4**

Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the source interface network (the real source address and the mapped destination address). See the following figure for an example of the original packet vs. the translated packet.

**a.** For **Match Criteria: Original Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Source Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. The default is **any**.

**b.** (Optional) For **Match Criteria: Original Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Destination Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
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, page 5-4.

**Step 5**

Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network (the *mapped source address* and the *real destination address*). You can translate between IPv4 and IPv6 if desired.

a. For **Action: Translated Packet > Source Address**, click the browse button and choose an existing network object that defines a host address, or an interface, or create a new object from the Browse Translated Source Address dialog box.

If you want to use the IPv6 address of the interface, check the Use IPv6 for interface PAT check box.

b. For **Action: Translated Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Translated Destination Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

For identity NAT for the destination address, simply use the same object or group for both the real and mapped addresses.

If you want to translate the destination address, then 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, page 5-38. See Guidelines for NAT, page 5-6 for information about disallowed mapped IP addresses.

For static interface NAT with port translation only, choose an interface from the Browse dialog box. Be sure to also configure a service translation. For this option, you must configure a specific interface for the Source Interface. See Static Interface NAT with Port Translation, page 5-40 for more information.

**Step 6**

(Optional.) Identify the destination service ports for service translation.

- Identify the original packet port (the *mapped destination port*). For **Match Criteria: Original Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Original Service dialog box.
• Identify the translated packet port (the real destination port). For Action: Translated Packet > Service, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Translated Service dialog box.

Dynamic NAT does not support port translation. However, because the destination translation is always static, you can perform port translation for the destination port. 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. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports. The “not equal” (!=) operator is not supported.

For example:
Step 7  (Optional) Configure NAT options in the Options area.

- **Enable rule**—Enables this NAT rule. The rule is enabled by default.
- (For a source-only rule.) **Translate DNS replies that match this rule**—Rewrites the DNS A record in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). You cannot configure DNS modification if you configure a destination address. See DNS and NAT, page 6-39 for more information.
- **Description**—Adds a description about the rule up to 200 characters in length.

Step 8  Click OK, then click Apply.

### Configure Dynamic Twice PAT Using a PAT Pool

This section describes how to configure twice NAT for dynamic PAT using a PAT pool.

**Procedure**

**Step 1**  Choose Configuration > Firewall > NAT Rules, and then do one of the following:

- Click Add, or Add > Add NAT Rule Before Network Object NAT Rules.
- Click Add > Add NAT Rule After Network Object NAT Rules.
- Select a twice NAT rule and click Edit.

The Add NAT Rule dialog box appears.
Chapter 5  Network Address Translation (NAT)

Dynamic PAT

Step 2  Set the source and destination interfaces.

By default in routed mode, both interfaces are set to --Any--. In transparent firewall mode, you must set specific interfaces.

a.  From the Match Criteria: Original Packet > Source Interface drop-down list, choose the source interface.

b.  From the Match Criteria: Original Packet > Destination Interface drop-down list, choose the destination interface.

Step 3  Choose Dynamic from the Action: Translated Packet > Source NAT Type drop-down list.

This setting only applies to the source address; the destination translation is always static.
Step 4  Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the source interface network (the real source address and the mapped destination address). See the following figure for an example of the original packet vs. the translated packet.

![Diagram showing original and translated packet addresses]

a. For the **Match Criteria: Original Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Source Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. The default is any.

b. (Optional.) For the **Match Criteria: Original Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Destination Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

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](#), page 5-4.

Step 5  Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network (the mapped source address and the real destination address). You can translate between IPv4 and IPv6 if desired.

a. Check the **PAT Pool Translated Address** check box, then click the browse button and choose an existing network object or group or create a new object or group from the Browse Translated PAT Pool Address dialog box. **Note:** Leave the Source Address field empty.

![PAT Pool Translated Address configuration screen]

**Note**  The object or group cannot contain a subnet.
b. For **Action: Translated Packet > Destination Address**, click the browse button and choose an existing network object, group, or interface or create a new object or group from the Browse Translated Destination Address dialog box.

For identity NAT for the destination address, simply use the same object or group for both the real and mapped addresses.

If you want to translate the destination address, then 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, page 5-38. See Guidelines for NAT, page 5-6 for information about disallowed mapped IP addresses.

For static interface NAT with port translation only, choose an interface from the Browse dialog box. Be sure to also configure a service translation. For this option, you must configure a specific interface for the Source Interface. See Static Interface NAT with Port Translation, page 5-40 for more information.

**Step 6** (Optional.) Identify the destination service ports for service translation.

- Identify the original packet port (the *mapped destination port*). For **Match Criteria: Original Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Original Service dialog box.

- Identify the translated packet port (the *real destination port*). For **Action: Translated Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Translated Service dialog box.

Dynamic NAT does not support port translation. However, because the destination translation is always static, you can perform port translation for the destination port. 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. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports. The “not equal” (\(!=\) operator is not supported.

For example:
Step 7  (Optional.) For a PAT pool, configure the following options:

- To assign addresses/ports in a round-robin fashion, check the **Round Robin** check box. 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.

- (8.4(3) and later, not including 8.5(1) or 8.6(1)) Check the **Extend PAT uniqueness to per destination instead of per interface** check box to use extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

- (8.4(3) and later, not including 8.5(1) or 8.6(1)) Check the **Translate TCP or UDP ports into flat range (1024-65535)** check box to use the 1024 to 65535 port range as a single flat 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 check the **Include range 1 to 1023** check box.
Step 8  (Optional, Routed Mode Only.) To use the interface IP address as a backup method if the other mapped source addresses are already allocated, check the **Fall through to interface PAT** check box. To use the IPv6 interface address, also check the **Use IPv6 for interface PAT** check box.

The destination interface IP address is used. This option is only available if you configure a specific Destination Interface.

![Dynamic PAT Configuration](image)

Step 9  (Optional.) Configure NAT options in the Options area.

- **Enable rule** — Enables this NAT rule. The rule is enabled by default.
- (For a source-only rule) **Translate DNS replies that match this rule** — Rewrites the DNS A record in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). You cannot configure DNS modification if you configure a destination address. See DNS and NAT, page 6-39 for more information.
- **Description** — Adds a description about the rule up to 200 characters in length.

**Step 10**  Click **OK**, then click **Apply**.

---

**Configure Per-Session PAT or Multi-Session PAT (Version 9.0(1) and Higher)**

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 $65535/\text{average-lifetime}$.

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. These rules are available starting with version 9.0(1).

**Before You Begin**

By default, the following rules are installed:

- Permit TCP from any (IPv4 and IPv6) to any (IPv4 and IPv6).
- Permit UDP from any (IPv4 and IPv6) to the domain port.

These rules do not show up in the table.

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:

- Deny TCP from any (IPv4 and IPv6) to any (IPv4 and IPv6).
- Deny UDP from any (IPv4 and IPv6) to the domain port.

**Procedure**

**Step 1** Choose Configuration > Firewall > Advanced > Per-Session NAT Rules.

**Step 2** Do one of the following:

- Choose Add > Add Per-Session NAT Rule.
- Select a rule and click Edit.

**Step 3** Configure the rule:

- **Action**—Click Permit or Deny. A permit rule uses per-session PAT; a deny rule uses multi-session PAT.
- **Source**—Specify the Source Address either by typing an address or clicking the ... button to choose an object. For the service, select UDP or TCP. You can optionally specify a source port, although normally you only specify the destination port. Either type in UDP//port or TCP//port, or click the ... button to select a common value or object.
- **Destination**—Specify the Destination Address either by typing an address or clicking the ... button to choose an object. For the service, select UDP or TCP; this must match the source service. You can optionally specify a destination port. Either type in UDP//port or TCP//port, or click the ... button to select a common value or object. You can use the operators != (not equal to), > (greater than), < (less than), or specify a range using a hyphen, for example, 100-200.

**Step 4** Click OK, then click Apply.
Static NAT

The following topics explain static NAT and how to implement it.

- About Static NAT, page 5-38
- Configure Static Network Object NAT or Static NAT-with-Port-Translation, page 5-43
- Configure Static Twice NAT or Static NAT-with-Port-Translation, page 5-45

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.

![Static NAT figure]

**Note**

You can disable bidirectionality if desired.

Static NAT with Port Translation

Static NAT with port translation lets you specify a real and mapped protocol (TCP or UDP) and port.

- About Static NAT with Port Address Translation, page 5-38
- Static NAT with Identity Port Translation, page 5-39
- Static NAT with Port Translation for Non-Standard Ports, page 5-40
- Static Interface NAT with Port Translation, page 5-40

About Static NAT with Port Address Translation

When you specify the port with static NAT, you can choose to map the port and/or the IP address to the same value or to a different value.
The following figure shows a typical static NAT with port translation scenario showing both a port that is mapped to itself and a port that is mapped to a different value; the IP address is mapped to a different value in both cases. The translation is always active so both translated and remote hosts can initiate connections.

**Figure 5-6  Typical Static NAT with Port Translation Scenario**

<table>
<thead>
<tr>
<th>Inside</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.2:8080</td>
<td>209.165.201.2:80</td>
</tr>
<tr>
<td>10.1.1.1:23</td>
<td>209.165.201.1:23</td>
</tr>
</tbody>
</table>

*Note*

For applications that require application inspection for secondary channels (for example, FTP and VoIP), the ASA automatically translates the secondary ports.

**Static NAT with Identity 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.
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 ASA outside interface to an inside host, then you can map the inside host IP address/port 23 to the ASA interface address/port 23. (Note that although Telnet to the ASA is not allowed to the lowest security interface, static NAT with interface port translation redirects the Telnet session instead of denying it).

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/1st mapped IP is technically the only bidirectional translation.

**Figure 5-8 One-to-Many Static NAT**

For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server.

**Figure 5-9 One-to-Many Static NAT Example**

Other Mapping Scenarios (Not Recommended)

The ASA 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 5-10 Few-to-Many Static NAT](image)

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 5-11 Many-to-Few Static NAT](image)

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 Add NAT to a new or existing network object:
- To add a new network object, choose Configuration > Firewall > NAT Rules, then click Add > Add Network Object NAT Rule.
- To add NAT to an existing network object, choose Configuration > Firewall > Objects > Network Objects/Groups, and then edit a network object.

Step 2 For a new object, enter values for the following fields:
- **Name**—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.
- **Type**—Host, Network, or Range.
- **IP Addresses**—IPv4 or IPv6 addresses, a single address for a host, a starting and ending address for a range, and for subnet, either an IPv4 network address and mask (for example, 10.100.10.0 255.255.255.0) or IPv6 address and prefix length (for example, 2001:DB8:0:CD30::/60).

Step 3 If the NAT section is hidden, click NAT to expand the section.

Step 4 Check the **Add Automatic Translation Rules** check box.

Step 5 From the Type drop-down list, choose **Static**.
Step 6 In the Translated Addr. field, 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. For more information, see Static NAT, page 5-38.

- Type an IP address.

  When you type an IP address, the netmask, prefix, or range for the mapped network is the same as that of the real network. For example, if the real network is a host, then this address will be a host address. In the case of a range, then the mapped addresses include the same number of addresses as the real range. For example, if the real address is defined as a range from 10.1.1.1 through 10.1.1.6, and you specify 172.20.1.1 as the mapped address, then the mapped range will include 172.20.1.1 through 172.20.1.6.

- Click the browse button and select a network object (or create a new one).

- (For static NAT-with-port-translation only; routed mode only.) Type an interface name or click the browse button, and choose an interface from the Browse Translated Addr dialog box.

To use the IPv6 interface address, you must also check the Use IPv6 for interface PAT check box. Be sure to also click Advanced and configure a service port translation. (You cannot specify an interface in transparent mode.)
Chapter 5  Network Address Translation (NAT)

Static NAT

Step 7  (Optional.) For NAT46, check **Use one-to-one address translation.** For NAT 46, specify one-to-one 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.

Step 8  (Optional) Click **Advanced**, configure the following options in the Advanced NAT Settings dialog box, and click **OK**.

- **Translate DNS replies for rule**—Translates the IP address in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). See **DNS and NAT, page 6-39** for more information.

- **Disable Proxy ARP on egress interface**—Disables 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, page 6-30**.

- (Required for Transparent Firewall Mode.) **Interface**—Specifies the real interface (**Source**) and the mapped interface (**Destination**) where this NAT rule applies. By default, the rule applies to all interfaces.

- **Service**—Configures static NAT-with-port-translation. Choose **tcp** or **udp**, then enter the real port and the mapped port. You can use port numbers or a well-known port name such as ftp.

Step 9  Click **OK**, and then **Apply**.

Because static rules are bidirectional (allowing initiation to and from the real host), the NAT Rules table shows two rows for each static rule, one for each direction.

---

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  Choose **Configuration > Firewall > NAT Rules**, and then do one of the following:

- Click **Add**, or **Add > Add NAT Rule Before Network Object NAT Rules**.
- Click **Add > Add NAT Rule After Network Object NAT Rules**.
- Select a twice NAT rule and click **Edit**.

The Add NAT Rule dialog box appears.
**Static NAT**

**Step 2**  Set the source and destination interfaces.

By default in routed mode, both interfaces are set to --Any--. In transparent firewall mode, you must set specific interfaces.

a. From the **Match Criteria: Original Packet > Source Interface** drop-down list, choose the source interface.

b. From the **Match Criteria: Original Packet > Destination Interface** drop-down list, choose the destination interface.

**Step 3**  Choose **Static** from the **Action: Translated Packet > Source NAT Type** drop-down list. Static is the default setting.

This setting only applies to the source address; the destination translation is always static.
### Step 4

Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the source interface network (the *real source address* and the *mapped destination address*). See the following figure for an example of the original packet vs. the translated packet.

![Example of Original Packet vs. Translated Packet](image)

**a.** For **Match Criteria: Original Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Source Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. The default is any, but do not use this option except for identity NAT.

**b.** (Optional) For **Match Criteria: Original Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Destination Address dialog box.

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, page 5-4.

### Step 5

Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network (the *mapped source address* and the *real destination address*). You can translate between IPv4 and IPv6 if desired.

**a.** For **Action: Translated Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Translated Source Address dialog box.

For static NAT, the 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, you can specify the interface instead of a network object/group for the mapped address. If you want to use the IPv6 address of the interface, check the **Use IPv6 for interface PAT** check box.
For more information, see Static Interface NAT with Port Translation, page 5-40. See Guidelines for NAT, page 5-6 for information about disallowed mapped IP addresses.

b. (Optional.) For Action: Translated Packet > Destination Address, click the browse button and choose an existing network object or group, or create a new object or group from the Browse Translated Destination Address dialog box.

Step 6  (Optional.) Identify the source or destination service ports for service translation.

- Identify the original packet source or destination port (the real source port or the mapped destination port). For Match Criteria: Original Packet > Service, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Original Service dialog box.

- Identify the translated packet source or destination port (the mapped source port or the real destination port). For Action: Translated Packet > Service, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Translated Service dialog box.

A service object can contain both a source and destination port. You should specify either the source or the destination port for both the real and mapped 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. In the rare case where you specify both the source and destination ports in the object, the original packet service object contains the real source port/mapped destination port; the translated packet service object contains the mapped source port/real destination port. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports. The “not equal” (≠) operator is not supported.

For example:
Step 7  (Optional.) For NAT46, check the **Use one-to-one address translation** check box. For NAT46, specify one-to-one 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.

Step 8  (Optional.) Configure NAT options in the Options area.

- **Enable rule** — Enables this NAT rule. The rule is enabled by default.
- (For a source-only rule.) **Translate DNS replies that match this rule** — Rewrites the DNS A record in DNS replies. Be sure DNS inspection is enabled (it is enabled by default). You cannot configure DNS modification if you configure a destination address. See **DNS and NAT**, page 6-39 for more information.
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 5-12 Identity NAT**

The following topics explain how to configure identity NAT.

- Configure Identity Network Object NAT, page 5-50
- Configure Identity Twice NAT, page 5-52

### Configure Identity Network Object NAT

This section describes how to configure an identity NAT rule using network object NAT.

**Procedure**

**Step 1** Add NAT to a new or existing network object:

- To add a new network object, choose Configuration > Firewall > NAT Rules, then click Add > Add Network Object NAT Rule.
- To add NAT to an existing network object, choose Configuration > Firewall > Objects > Network Objects/Groups, and then edit a network object.
Step 2 For a new object, enter values for the following fields:

a. **Name**—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.

b. **Type**—Host, Network, or Range.

c. **IP Addresses**—IPv4 or IPv6 addresses, a single address for a host, a starting and ending address for a range, and for subnet, either an IPv4 network address and mask (for example, 10.100.10.0 255.255.255.0) or IPv6 address and prefix length (for example, 2001:DB8:0:CD30::/60).

Step 3 If the NAT section is hidden, click **NAT** to expand the section.

Step 4 Check the **Add Automatic Translation Rules** check box.

Step 5 From the Type drop-down list, choose **Static**.

Step 6 In the Translated Addr. field, do one of the following:

- Type the same IP address that you used for the real address.

  When you type an IP address, the netmask, prefix, or range for the mapped network is the same as that of the real network. For example, if the real network is a host, then this address will be a host address. In the case of a range, then the mapped addresses include the same number of addresses as the real range. For example, if the real address is defined as a range from 10.1.1.1 through 10.1.1.6, and you specify 10.1.1.1 as the mapped address, then the mapped range will include 10.1.1.1 through 10.1.1.6.

- Click the browse button and select a network object (or create a new one).
Step 7  (Optional) Click Advanced, configure the following options in the Advanced NAT Settings dialog box, and click OK.

- **Translate DNS replies for rule**—Do not configure this option for identity NAT.
- **Disable Proxy ARP on egress interface**—Disables 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, page 6-30.
- *(Routed mode; interfaces specified.)* **Lookup route table to locate egress interface**—Determines the egress interface using a route lookup instead of using the interface specified in the NAT command. See Determining the Egress Interface, page 6-32 for more information.
- *(Required for Transparent Firewall Mode.)* **Interface**—Specifies the real interface (Source) and the mapped interface (Destination) where this NAT rule applies. By default, the rule applies to all interfaces.
- **Service**—Do not configure this option for identity NAT.

Step 8  Click OK, and then Apply.

Because static rules are bidirectional (allowing initiation to and from the real host), the NAT Rules table shows two rows for each static rule, one for each direction, unless you select the route lookup option.

### Configure Identity Twice NAT

This section describes how to configure an identity NAT rule using twice NAT.

**Procedure**

**Step 1**  Choose Configuration > Firewall > NAT Rules, and then do one of the following:

- Click Add, or Add > Add NAT Rule Before Network Object NET Rules.
- Click Add > Add NAT Rule After Network Object NET Rules.
- Select a twice NAT rule and click Edit.

The Add NAT Rule dialog box appears.
Identity NAT

Step 2  Set the source and destination interfaces.

By default in routed mode, both interfaces are set to --Any--. In transparent firewall mode, you must set specific interfaces.

a. From the Match Criteria: Original Packet > Source Interface drop-down list, choose the source interface.

b. From the Match Criteria: Original Packet > Destination Interface drop-down list, choose the destination interface.

Step 3  Choose Static from the Action: Translated Packet > Source NAT Type drop-down list. Static is the default setting.

This setting only applies to the source address; the destination translation is always static.

Step 4  Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the source interface network (the real source address and the mapped destination address). See the following figure for an example of the original packet vs. the translated packet where you perform identity NAT on the inside host but translate the outside host.
Identity NAT

a. For **Match Criteria: Original Packet > Source Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Source Address dialog box. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. The default is **any**; only use this option when also setting the mapped address to **any**.

b. (Optional.) For **Match Criteria: Original Packet > Destination Address**, click the browse button and choose an existing network object or group or create a new object or group from the Browse Original Destination Address dialog box.

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, page 5-4.

**Step 5** Identify the translated packet addresses; namely, the packet addresses as they appear on the destination interface network (the **mapped source address** and the **real destination address**).

a. For **Action: Translated Packet > Source Address**, click the browse button and choose the same network object or group from the Browse Translated Source Address dialog box that you chose for the real source address. Use **any** if you specified **any** for the real address.

b. For **Match Criteria: Translated Packet > Destination Address**, click the browse button and choose an existing network object, group, or interface or create a new object or group from the Browse Translated Destination Address dialog box.

For identity NAT for the destination address, simply use the same object or group for both the real and mapped addresses.

If you want to translate the destination address, then 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, page 5-38. See Guidelines for NAT, page 5-6 for information about disallowed mapped IP addresses.

For static interface NAT with port translation only, choose an interface. If you specify an interface, be sure to also configure a service translation. For more information, see Static Interface NAT with Port Translation, page 5-40.

**Step 6** (Optional.) Identify the source or destination service ports for service translation.
• Identify the original packet source or destination port (the real source port or the mapped destination port). For **Match Criteria: Original Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Original Service dialog box.

• Identify the translated packet source or destination port (the mapped source port or the real destination port). For **Action: Translated Packet > Service**, click the browse button and choose an existing service object that specifies TCP or UDP ports, or create a new object from the Browse Translated Service dialog box.

A service object can contain both a source and destination port. You should specify either the source or the destination port for both the real and mapped 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. In the rare case where you specify both the source and destination ports in the object, the original packet service object contains the real source port/mapped destination port; the translated packet service object contains the mapped source port/real destination port. NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports. The “not equal” (!=) operator is not supported.

For example:
Identity NAT

Chapter 5  Network Address Translation (NAT)

Step 7  (Optional) Configure NAT options in the Options area.

- **Enable rule** — Enables this NAT rule. The rule is enabled by default.
- (For a source-only rule.) **Translate DNS replies that match this rule** — Although this option is available if you do not configure a destination address, it is not applicable to identity NAT because you are translating the address to itself, so the DNS reply does not need modification.
- **Disable Proxy ARP on egress interface** — Disables proxy ARP for incoming packets to the mapped IP addresses. See Mapped Addresses and Routing, page 6-30 for more information.
- (Routed mode; interfaces specified.) **Lookup route table to locate egress interface** — Determines the egress interface using a route lookup instead of using the interface specified in the NAT command. See Determining the Egress Interface, page 6-32 for more information.
- **Direction** — To make the rule unidirectional, choose **Unidirectional**. The default is Both. Making the rule unidirectional prevents traffic from initiating connections to the real addresses. You might want to use this setting for testing purposes.
- **Description** — Adds a description about the rule up to 200 characters in length.
Monitoring NAT

You can view NAT related graphs from the following pages:

- **Monitoring > Properties > Connection Graphs > Xlates**—Select the Xlate Utilization graph to view the in-use and most-used xlates. This is equivalent to the `show xlate` command.

- **Monitoring > Properties > Connection Graphs > Perfmon**—Select the Xlate Perfmon graph to see NAT performance information. This is equivalent to the xlate information from the `show perfmon` command.

History for NAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Object NAT</td>
<td>8.3(1)</td>
<td>Configures NAT for a network object IP address(es). We introduced or modified the following screens: Configuration &gt; Firewall &gt; NAT Rules Configuration &gt; Firewall &gt; Objects &gt; Network Objects/Groups</td>
</tr>
<tr>
<td>Twice NAT</td>
<td>8.3(1)</td>
<td>Twice NAT lets you identify both the source and destination address in a single rule. We modified the following screen: Configuration &gt; Firewall &gt; NAT Rules.</td>
</tr>
</tbody>
</table>
### History for NAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity NAT configurable proxy ARP and route lookup</td>
<td>8.4(2)/8.5(1)</td>
<td>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 <code>nat 0 access-list</code> command) to 8.4(2) and later now includes the following keywords to disable proxy ARP and to use a route lookup: <code>no-proxy-arp</code> and <code>route-lookup</code>. The <code>unidirectional</code> 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 <code>no-proxy-arp</code> and <code>route-lookup</code> keywords, to maintain existing functionality. The <code>unidirectional</code> keyword is removed. We modified the following screens: Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object &gt; Advanced NAT Settings; Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule.</td>
</tr>
<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. We modified the following screens: Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit Network Object; Configuration &gt; Firewall &gt; NAT Rules &gt; Add/Edit NAT Rule.</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 screens. This feature is not available in 8.5(1) or 8.6(1).</td>
</tr>
</tbody>
</table>
### History for NAT

- **Flat range of PAT ports for a PAT pool**
  - **Platform Releases**: 8.4(3)
  - **Description**: 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 screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule.
  - *This feature is not available in 8.5(1) or 8.6(1).*

- **Extended PAT for a PAT pool**
  - **Platform Releases**: 8.4(3)
  - **Description**: 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 screens: Configuration > Firewall > NAT Rules > Add/Edit Network Object; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule.
  - *This feature is not available in 8.5(1) or 8.6(1).*
### History for NAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automatic NAT rules to translate a VPN peer’s local IP address back to the peer’s real IP address | 8.4(3) | 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).  
  ASDM does not support this command; enter the command using the Command Line Tool. |
| NAT support for IPv6 | 9.0(1) | NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6. Translating between IPv4 and IPv6 is not supported in transparent mode.  
  We modified the following screen: Configuration > Firewall > Objects > Network Objects/Group; Configuration > Firewall > NAT Rules. |
| NAT support for reverse DNS lookups | 9.0(1) | 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. |
Chapter 5  Network Address Translation (NAT)

History for NAT

Per-session PAT

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 screen: Configuration &gt; Firewall &gt; Advanced &gt; Per-Session NAT Rules.</td>
</tr>
</tbody>
</table>

Transactional Commit Model on NAT Rule Engine

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 NAT to the following screen: Configuration &gt; Device Management &gt; Advanced &gt; Rule Engine.</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, page 6-1
- Examples for Twice NAT, page 6-14
- NAT in Routed and Transparent Mode, page 6-27
- Routing NAT Packets, page 6-29
- NAT for VPN, page 6-33
- DNS and NAT, page 6-39

Examples for Network Object NAT

Following are some configuration examples for network object NAT.

- Providing Access to an Inside Web Server (Static NAT), page 6-1
- NAT for Inside Hosts (Dynamic NAT) and NAT for an Outside Web Server (Static NAT), page 6-4
- Inside Load Balancer with Multiple Mapped Addresses (Static NAT, One-to-Many), page 6-7
- Single Address for FTP, HTTP, and SMTP (Static NAT-with-Port-Translation), page 6-10

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.
Procedure

**Step 1**  Choose **Configuration > Firewall > NAT**.

**Step 2**  Choose **Add > Network Object NAT Rule**, name the new network object and define the web server host address.

**Step 3**  Configure static NAT for the object.
Step 4  Click **Advanced** and configure the real and mapped interfaces.

Step 5  Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.
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.

Figure 6-2 Dynamic NAT for Inside, Static NAT for Outside Web Server

Procedure

Step 1 Choose Configuration > Firewall > NAT.
Step 2 Choose Add > Network Object NAT Rule, name the new network object and define the inside network.
Step 3 Enable dynamic NAT for the inside network.
**Step 4** For the Translated Addr field, add a new network object for the dynamic NAT pool to which you want to translate the inside addresses by clicking the browse button.

a. Choose **Add > Network Object**, name the new object, define the range of addresses in the NAT pool, and click **OK**.

b. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.
Step 5  Click **Advanced** and configure the real and mapped interfaces.

![Advanced NAT Settings](image)

Step 6  Click **OK** to return to the Edit Network Object dialog box, click then click **OK** again to return to the NAT Rules table.

Step 7  Choose **Add > Network Object NAT Rule** and create an object for the outside web server.

![Add Network Object](image)

Step 8  Configure static NAT for the web server.
Chapter 6      NAT Examples and Reference

Examples for Network Object NAT

Step 9   Click Advanced and configure the real and mapped interfaces.

Step 10  Click OK to return to the Edit Network Object dialog box, click OK again, and then click Apply.

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.
**Procedure**

**Step 1** Choose Configuration > Firewall > NAT.

**Step 2** Choose Add > Network Object NAT Rule, name the new network object and define the load balancer address.

**Step 3** Enable static NAT for the load balancer:
Step 4  For the Translated Addr field, add a new network object for the static NAT group of addresses to which you want to translate the load balancer address by clicking the browse button.

a.  Choose Add > Network Object, name the new object, define the range of addresses, and click OK.

b.  Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.

Step 5  Click Advanced and configure the real and mapped interfaces.
Step 6  
Click OK to return to the Edit Network Object dialog box, click OK again, and then click Apply.

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 6-4** Static NAT-with-Port-Translation

**Procedure**

**Step 1** Choose **Configuration > Firewall > NAT**.

**Step 2** Configure the static network object NAT with port translation rule for the FTP server.

- **a.** Choose **Add > Network Object NAT Rule**.

- **b.** Name the new network object, define the FTP server address, enable static NAT, and enter the translated address.
c. Click **Advanced** and configure the real and mapped interfaces and port translation for FTP, mapping the FTP port to itself.

![Add Network Object](image1.png)

![Advanced NAT Settings](image2.png)

d. Click **OK**, then **OK** again to save the rule and return to the NAT page.

**Step 3** Configure the static network object NAT with port translation rule for the HTTP server.

a. Choose **Add > Network Object NAT Rule**.

b. Name the new network object, define the HTTP server address, enable static NAT, and enter the translated address.
c. Click **Advanced** and configure the real and mapped interfaces and port translation for HTTP, mapping the HTTP port to itself.

![Advanced NAT Settings](image)

**Step 4** Configure the static network object NAT with port translation rule for the SMTP server.

a. Choose **Add > Network Object NAT Rule**.

b. Name the new network object, define the SMTP server address, enable static NAT, and enter the translated address.
Examples for Twice NAT

This section includes the following configuration examples:

- Different Translation Depending on the Destination (Dynamic Twice PAT), page 6-15
- Different Translation Depending on the Destination Address and Port (Dynamic PAT), page 6-20
- Example: Twice NAT with Destination Address Translation, page 6-27
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 6-5  Twice NAT with Different Destination Addresses

Step 1

On the Configuration > Firewall > NAT Rules page, click Add > Add NAT Rule Before Network Object NAT Rules to add a NAT rule for traffic from the inside network to DMZ network 1.

If you want to add a NAT rule to section 3, after the network object NAT rules, choose Add NAT Rule After Network Object NAT Rules.

The Add NAT Rule dialog box appears.
Step 2  Set the source and destination interfaces.

Step 3  For the Original Source Address, click the browse button to add a new network object for the inside network in the Browse Original Source Address dialog box.
   a. Select Add > Network Object.
   b. Define the inside network addresses, and click OK.
   c. Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.

Step 4  For the Original Destination Address, click the browse button to add a new network object for DMZ network 1 in the Browse Original Destination Address dialog box.
   a. Select Add > Network Object.
b. Define the DMZ network 1 addresses, and click **OK**.

![Add Network Object](image1)

C. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.

![Selected Original Destination Address](image2)

**Step 5** Set the NAT Type to **Dynamic PAT (Hide)**:

![Edit NAT Rule](image3)

**Step 6** For the Translated Source Address, click the browse button to add a new network object for the PAT address in the Browse Translated Source Address dialog box.

a. Select **Add > Network Object**.

b. Define the PAT address, and click **OK**.

![Add Network Object](image4)

c. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.
Step 7 For the Translated Destination Address, type the name of the Original Destination Address (DMZnetwork1) or click the browse button to choose it.

Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the Original and Translated destination addresses.

Step 8 Click OK to add the rule to the NAT table.

Step 9 Click Add > Add NAT Rule Before Network Object NAT Rules or Add NAT Rule After Network Object NAT Rules to add a NAT rule for traffic from the inside network to DMZ network 2.

Step 10 Set the source and destination interfaces.

Step 11 For the Original Source Address, type the name of the inside network object (myInsideNetwork) or click the browse button to choose it.

Step 12 For the Original Destination Address, click the browse button to add a new network object for DMZ network 2 in the Browse Original Destination Address dialog box.

a. Select Add > Network Object.

b. Define the DMZ network 2 addresses, and click OK.
c. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.

**Step 13** Set the NAT Type to **Dynamic PAT (Hide)**:

**Step 14** For the Translated Source Address, click the browse button to add a new network object for the PAT address in the Browse Translated Source Address dialog box.

a. Select **Add > Network Object**.

b. Define the PAT address, and click **OK**.

c. Choose the new network object by double-clicking it. Click **OK** to return to the NAT configuration.
Step 15 For the Translated Destination Address, type the name of the Original Destination Address (DMZnetwork2) or click the browse button to choose it.

Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the Original and Translated destination addresses.

Step 16 Click OK to add the rule to the NAT table.

Step 17 Click Apply.

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.
Examples for Twice NAT

Figure 6-6  Twice NAT with Different Destination Ports

Step 1 On the Configuration > Firewall > NAT Rules page, click Add > Add NAT Rule Before Network Object NAT Rules to add a NAT rule for traffic from the inside network to the Telnet server.

If you want to add a NAT rule to section 3, after the network object NAT rules, choose Add NAT Rule After Network Object NAT Rules.

The Add NAT Rule dialog box appears.

Step 2 Set the source and destination interfaces.
Step 3  For the Original Source Address, click the browse button to add a new network object for the inside network in the Browse Original Source Address dialog box.

a. Select Add > Network Object.

b. Define the inside network addresses, and click OK.

c. Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.

Step 4  For the Original Destination Address, click the browse button to add a new network object for the Telnet/Web server in the Browse Original Destination Address dialog box.

a. Select Add > Network Object.

b. Define the server address, and click OK.

c. Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.
Step 5  For the Original Service, click the browse button to add a new service object for Telnet in the Browse Original Service dialog box.
   a. Select Add > Service Object.
   b. Define the protocol and port, and click OK.
   c. Choose the new service object by double-clicking it. Click OK to return to the NAT configuration.

Step 6  Set the NAT Type to **Dynamic PAT (Hide)**:

Step 7  For the Translated Source Address, click the browse button to add a new network object for the PAT address in the Browse Translated Source Address dialog box.
   a. Select Add > Network Object.
   b. Define the PAT address, and click OK.
c. Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.

Step 8 For the Translated Destination Address, type the name of the Original Destination Address (TelnetWebServer) or click the browse button to choose it.

Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the Original and Translated destination addresses.

Step 9 Click OK to add the rule to the NAT table.

Step 10 Click Add > Add NAT Rule Before Network Object NAT Rules or Add NAT Rule After Network Object NAT Rules to add a NAT rule for traffic from the inside network to the web server.

Step 11 Set the real and mapped interfaces.
Step 12  For the Original Source Address, type the name of the inside network object (myInsideNetwork) or click the browse button to choose it.

Step 13  For the Original Destination Address, type the name of the Telnet/web server network object (TelnetWebServer) or click the browse button to choose it.

Step 14  For the Original Service, click the browse button to add a new service object for HTTP in the Browse Original Service dialog box.

a. Select **Add > Service Object**.

b. Define the protocol and port, and click **OK**.

c. Choose the new service object by double-clicking it. Click **OK** to return to the NAT configuration.

Step 15  Set the NAT Type to **Dynamic PAT (Hide)**:

Step 16  For the Translated Source Address, click the browse button to add a new network object for the PAT address in the Browse Translated Source Address dialog box.

a. Select **Add > Network Object**.

b. Define the PAT address, and click **OK**.
c. Choose the new network object by double-clicking it. Click OK to return to the NAT configuration.

**Step 17** For the Translated Destination Address, type the name of the Original Destination Address (TelnetWebServer) or click the browse button to choose it.

Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the Original and Translated destination addresses.

**Step 18** Click OK to add the rule to the NAT table.

**Step 19** Click Apply.
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 6-7  Twice Static NAT with Destination Address Translation

NAT in Routed and Transparent Mode

You can configure NAT in both routed and transparent firewall mode. This section describes typical usage for each firewall mode.

- NAT in Routed Mode, page 6-28
- NAT in Transparent Mode, page 6-28
**NAT in Routed Mode**

The following figure shows a typical NAT example in routed mode, with a private network on the inside.

*Figure 6-8  NAT Example: Routed Mode*

1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is changed 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**

Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks.

NAT in transparent mode has the following requirements and limitations:

- Because the transparent firewall does not have any interface IP addresses, you cannot use interface PAT.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the 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. See Mapped Addresses and Routing, page 6-30 for more information about required routes.

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. See Transparent Mode Routing Requirements for Remote Networks, page 6-32 for more information about required routes.

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, page 6-30
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, page 5-8.

The following topics explain the mapped address types:

- Addresses on the Same Network as the Mapped Interface, page 6-30
- Addresses on a Unique Network, page 6-30
- The Same Address as the Real Address (Identity NAT), page 6-31

Addresses on the Same Network as the Mapped Interface

If you use addresses on the same network as the 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 (see Configuration > Device Management > Advanced > ARP > ARP Static Table). 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.

Addresses on a Unique Network

If you need more addresses than are available on the mapped interface network, you can identify addresses on a different subnet. The 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 the following static route 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: in 8.3, specify the global management IP address; in 8.4(1) and later, 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)

(8.3(1), 8.3(2), and 8.4(1)) The default behavior for identity NAT has proxy ARP disabled. You cannot configure this setting.

(8.4(2) and later) 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 (see the following figure).

**Figure 6-10 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).
Routing NAT Packets

Figure 6-11  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 the ASA receives traffic for a mapped address, 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:

- Transparent mode—The ASA determines the egress interface for the real address by using the NAT rule; you must specify the source and destination interfaces as part of the NAT rule.
- 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. (8.3(1) through 8.4(1)) The only exception is for identity NAT, which always uses a route lookup, regardless of the NAT configuration. (8.4(2) and later) For identity NAT, the default behavior is to use the NAT configuration. However, you have the option to always use a route lookup instead. In certain scenarios, a route lookup override is required; for example, see NAT and VPN Management Access, page 6-37.
  - 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.
NAT for VPN

The following topics explain NAT usage with the various types of VPN.

- NAT and Remote Access VPN, page 6-33
- NAT and Site-to-Site VPN, page 6-35
- NAT and VPN Management Access, page 6-37
- Troubleshooting NAT and VPN, page 6-39

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 client 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).
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:

```plaintext
! 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.
The following figure shows a VPN client connected to ASA1 (Boulder), with a Telnet request for a server (10.2.2.78) accessible over a site-to-site tunnel between ASA1 and ASA2 (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.

The following sample NAT configuration for ASA1 (Boulder):

```plaintext
! 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 VPN client and San Jose without
! address translation (identity NAT):
  nat (outside,outside) source static vpn_local vpn_local destination static sanjose_inside
  sanjose_inside

See the following sample NAT configuration for ASA2 (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. 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, page 6-33 or NAT and Site-to-Site VPN, page 6-35, 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, page 6-32 for more information about the route lookup option.

![Figure 6-17 VPN Management Access](image)

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
```
DNS and NAT

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`.

DNS and 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.

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 some limitations with DNS rewrite:

- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record, and the PAT rule to use is ambiguous.
- If you configure a twice NAT rule, you cannot configure DNS modification if you specify the source address as well as the destination 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.
- DNS rewrite requires DNS application inspection to be enabled, which it is on by default. See DNS Inspection, page 8-1 for more information.
- 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.

! 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
```
The following topics provide examples of DNS rewrite:

- DNS Reply Modification, DNS Server on Outside, page 6-40
- DNS Reply Modification, DNS Server, Host, and Server on Separate Networks, page 6-42
- DNS Reply Modification, DNS Server on Host Network, page 6-43
- DNS64 Reply Modification Using Outside NAT, page 6-45
- PTR Modification, DNS Server on Host Network, page 6-50

**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 the ASA 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 ASA 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.
Figure 6-18  DNS Reply Modification, DNS Server on Outside

**Procedure**

**Step 1**  Choose Configuration > Firewall > NAT.

**Step 2**  Choose Add > Network Object NAT Rule.

**Step 3**  Name the new network object, define the FTP server address, enable static NAT and enter the translated address.
Step 4  Click **Advanced** and configure the real and mapped interfaces and DNS modification.

Step 5  Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

### 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 6-19  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 ASA has a static translation for the outside server. In this case, when an inside user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.20.10. Because you want inside users to use the mapped address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.
Figure 6-20 DNS Reply Modification, DNS Server on Host Network

Procedure

Step 1 Choose Configuration > Firewall > NAT.
Step 2 Choose Add > Network Object NAT Rule.
Step 3 Name the new network object, define the FTP server address, enable static NAT and enter the translated address.
DNS and NAT

Step 4  Click **Advanced** and configure the real and mapped interfaces and DNS modification.

Step 5  Click **OK** to return to the Edit Network Object dialog box, click **OK** again, and then click **Apply**.

DNS64 Reply Modification Using Outside NAT

The following figure shows an FTP server and DNS server on the outside IPv4 network. The ASA 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) 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** Choose **Configuration > Firewall > NAT.**

**Step 2** Configure static network object NAT with DNS modification for the FTP server.

a. Choose **Add > Network Object NAT Rule.**

b. Name the new network object, define the FTP server address, enable static NAT, and enter the translated address. Because this is a one-to-one translation for NAT46, select **Use one-to-one address translation.**
c. Click **Advanced** to configure the real and mapped interfaces and DNS modification.

d. Click **OK** to return to the Network Object dialog box, and click **OK** again to save the rule.

**Step 3** Configure static network object NAT for the DNS server.

a. Choose **Add > Network Object NAT Rule**.
b. Name the new network object, define the DNS server address, enable static NAT, and enter the translated address. Because this is a one-to-one translation for NAT46, select **Use one-to-one address translation.**

![Add Network Object](image)

![Advanced NAT Settings](image)

c. Click **Advanced** to configure the real and mapped interfaces.

d. Click **OK** to return to the Network Object dialog box, and click **OK** again to save the rule.

**Step 4** Configure PAT for the inside IPv6 network.

a. Choose **Add > Network Object NAT Rule.**

b. Name the new network object, define the IPv6 network address, and select **Dynamic** NAT.

c. Select **PAT Pool Translated Address**, and click the ... (browse) button to create the PAT pool object.

d. In the Browse PAT Pool Translated Address dialog box, select **Add > Network Object**. Name the new object, enter the address range for the PAT pool, and click **OK**.

e. In the Browse PAT Pool Translated Address dialog box, double-click the PAT pool object you created to select it and click OK.

f. Click Advanced to configure the real and mapped interfaces.

g. Click OK to return to the Network Object dialog box.
Step 5  Click OK, and then click Apply.

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 6-22  PTR Modification, DNS Server on Host Network

ftp.cisco.com
209.165.201.10
Static Translation on Inside to:
10.1.2.56

DNS Server

Reverse DNS Query
209.165.201.10

Reverse DNS Query Modification
10.1.2.56 → 209.165.201.10

PTR Record
ftp.cisco.com

Outside

ASA

Inside

User
10.1.2.27

Reverse DNS Query
10.1.2.56?

304002
PART 3

Application Inspection
Getting Started with Application Layer Protocol Inspection

The following topics describe how to configure application layer protocol inspection.

- Application Layer Protocol Inspection, page 7-1
- Guidelines for Application Inspection, page 7-4
- Defaults for Application Inspection, page 7-5
- Configure Application Layer Protocol Inspection, page 7-8
- Configure Regular Expressions, page 7-11
- History for Application Inspection, page 7-15

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 (see the general operations configuration guide for more information about 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.

- How Inspection Engines Work, page 7-1
- When to Use Application Protocol Inspection, page 7-2
- Inspection Policy Maps, page 7-3

How Inspection Engines Work

As illustrated in the following figure, the ASA uses three databases for its basic operation:

- ACLs—Used for authentication and authorization of connections based on specific networks, hosts, and services (TCP/UDP port numbers).
- Inspections—Contains a static, predefined set of application-level inspection functions.
Connections (XLATE and CONN tables)—Maintains state and other information about each established connection. This information is used by the Adaptive Security Algorithm and cut-through proxy to efficiently forward traffic within established sessions.

**Figure 7-1  How Inspection Engines Work**

In this figure, operations are numbered in the order they occur:

1. A TCP SYN packet arrives at the ASA to establish a new connection.
2. The ASA checks the ACL database to determine if the connection is permitted.
3. The ASA creates a new entry in the connection database (XLATE and CONN tables).
4. The ASA checks the Inspections database to determine if the connection requires application-level inspection.
5. After the application inspection engine completes any required operations for the packet, the ASA forwards the packet to the destination system.
6. The destination system responds to the initial request.
7. The ASA receives the reply packet, looks up the connection in the connection database, and forwards the packet because it belongs to an established session.

The default configuration of the ASA includes a set of application inspection entries that associate supported protocols with specific TCP or UDP port numbers and that identify any special handling required.

**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.

See [Configure Application Layer Protocol Inspection](#) for a list of applications that support inspection policy maps.

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](#)
- [How Multiple Traffic Classes are Handled](#)

### Replacing an In-Use Inspection Policy Map

If you need to replace an inspection policy map that you are already using in a service policy, use the following methods:

- All inspection policy maps—If you want to exchange an in-use inspection policy map for a different map name, you must remove, apply changes, and add the new inspection policy map back to the service policy.
Guidelines for Application Inspection

Failover Guidelines
State information for multimedia sessions that require inspection are not passed over the state link for stateful failover. The exceptions are GTP and SIP, which are replicated over the state link.

IPv6 Guidelines
Supports IPv6 for the following inspections:
- DNS
- FTP
- HTTP
- ICMP
- SCCP (Skinny)
- SIP
- SMTP
- IPsec pass-through
- IPv6

Supports NAT64 for the following inspections:
- DNS
• FTP
• HTTP
• ICMP

Additional Guidelines and Limitations

• 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, page 7-5.

• 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.

• 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, page 7-5
• Default Inspection Policy Maps, page 7-8

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 7-1 Supported Application Inspection Engines

<table>
<thead>
<tr>
<th>Application Group</th>
<th>Default Port</th>
<th>NAT Limitations</th>
<th>Standards</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CTIQBE            | TCP/2748     | No extended PAT.  
                | No NAT64.  
                | —          | —        |
| DCERPC            | TCP/135      | No NAT64.  
                | —          | —        |
| DNS over UDP      | UDP/53       | No NAT support is available for name resolution through WINS.  
                | RFC 1123   | —        |
| FTP               | TCP/21       | (Clustering) No static PAT.  
                | RFC 959    | —        |
| GTP               | UDP/3386     | No extended PAT.  
                | —          | Requires a special license. |
|                   | UDP/2123     | No extended PAT.  
                | —          | —        |
| H.323 H.225 and RAS | TCP/1720  
                  | UDP/1718  
                  | UDP (RAS)  
                  | 1718-1719 | No dynamic NAT or PAT.  
                | No extended PAT.  
                | Static PAT may not work.  
                | (Clustering) No static PAT.  
                | No extended PAT.  
                | No per-session PAT.  
                | No NAT on same security interfaces.  
                | No NAT64.  
                | ITU-T H.323,  
                | H.245, H225.0,  
                | Q.931, Q.932 | —        |
| HTTP              | TCP/80       | —          | RFC 2616 | Beware of MTU limitations stripping ActiveX and Java. If the MTU is too small to allow the Java or ActiveX tag to be included in one packet, stripping may not occur. |
| ICMP              | —            | —          | —         | ICMP traffic directed to an ASA interface is never inspected. |
| ICMP ERROR        | —            | —          | —         | —        |
| ILS (LDAP)        | TCP/389      | No extended PAT.  
                | —          | —        |
| Instant Messaging (IM) | Varies by client | No extended PAT.  
                | RFC 3860   | —        |
| IP Options        | —            | No NAT64.  
                | RFC 791, RFC 2113 | —        |
| IPsec Pass Through | UDP/500 | No PAT.  
                | —          | —        |
| IPv6              | —            | No NAT64.  
                | RFC 2460   | —        |
| MGCP              | UDP/2427, 2727 | No extended PAT.  
                | RFC 2705bis-05 | —        |
|                   |              | No NAT64.  
                | —          | —        |
|                   |              | (Clustering) No static PAT.  
                | —          | —        |
### Table 7-1  Supported Application Inspection Engines (continued)

<table>
<thead>
<tr>
<th>Application</th>
<th>Default Port</th>
<th>NAT Limitations</th>
<th>Standards</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMP</td>
<td>TCP 5443</td>
<td>No extended PAT. 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. No NAT64.</td>
<td>—</td>
<td>NetBIOS is supported by performing NAT of the packets for NBNS UDP port 137 and NBDS UDP port 138.</td>
</tr>
<tr>
<td>PPTP</td>
<td>TCP/1723</td>
<td>No NAT64.       (Clustering) No static PAT.</td>
<td>RFC 2637</td>
<td>—</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>1646</td>
<td>No NAT64.</td>
<td>RFC 2865</td>
<td>—</td>
</tr>
<tr>
<td>RSH</td>
<td>TCP/514</td>
<td>No PAT.         No NAT64. (Clustering) No static PAT.</td>
<td>Berkeley UNIX</td>
<td>—</td>
</tr>
<tr>
<td>RTSP</td>
<td>TCP/554</td>
<td>No extended PAT. No NAT64. (Clustering) No static PAT.</td>
<td>RFC 2326, 2327, 1889</td>
<td>No handling for HTTP cloaking.</td>
</tr>
<tr>
<td>ScanSafe (Cloud Web Security)</td>
<td>TCP/80 TCP/413</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>SIP</td>
<td>TCP/5060 UDP/5060</td>
<td>No NAT on same security interfaces. No extended PAT. No per-session 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 per-session 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</td>
<td>v.2 RFC 1902-1908; v.3 RFC 2570-2580.</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>
</tbody>
</table>
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; use Tools > Command Line Interface.

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. Service policies 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. For some applications, you can perform special actions when you enable inspection. See Chapter 1, “Service Policy,” for information about service policies in general.

Inspection is enabled by default for some applications. See Default Inspections and NAT Limitations, page 7-5 section for more information. Use this section to modify your inspection policy.

Procedure

Step 1 Choose Configuration > Firewall > Service Policy Rules.

Step 2 Add or edit a service policy rule according to Add a Service Policy Rule for Through Traffic, page 1-10, and proceed to the Rule Action page.

If you want to match non-standard ports, then create a new rule for the non-standard ports. See Default Inspections and NAT Limitations, page 7-5 for the standard ports for each inspection engine.
You can combine multiple rules in the same service policy if desired, so you can create one rule to match
certain traffic, and another to match different traffic. However, if traffic matches a rule that contains an
inspection action, and then matches another rule that also has an inspection action, only the first
matching rule is used.

If you are implementing RADIUS accounting inspection, create a management service policy rule

**Step 3**
In the rule actions, click the **Protocol Inspection** tab.

**Step 4**
(To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map,
you must disable the inspection, and then re-enable it with the new inspection policy map name:

a. Uncheck the protocol’s check box.
b. Click **OK**.
c. Click **Apply**.
d. Repeat these steps to return to the Protocol Inspections tab.

**Step 5**
Select the inspection type that you want to apply.

You can select multiple options on the default inspection traffic class only.

Some inspection engines let you control additional parameters when you apply the inspection to the
traffic. Click **Configure** for the inspection type to configure an inspection policy map. You can either
choose an existing map, or create a new one. You can predefine inspection policy maps from the
**Configuration > Firewall > Objects > Inspect Maps** list.

The following table lists the protocols you can inspect, whether they allow inspection policy maps or
inspection class maps, and a pointer to detailed information about the inspection.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supports Inspection Policy Maps</th>
<th>Supports Inspection Class Maps</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTIQBE</td>
<td>No</td>
<td>No</td>
<td>See CTIQBE Inspection, page 9-1.</td>
</tr>
<tr>
<td>Cloud Web Security</td>
<td>Yes</td>
<td>Yes</td>
<td>If you want to enable ScanSafe (Cloud Web Security), use the procedure described in the following topic rather than this procedure: Configure a Service Policy to Send Traffic to Cloud Web Security, page 15-9. The cited procedure explains the full policy configuration, including how to configure the policy inspection map.</td>
</tr>
<tr>
<td>DCERPC</td>
<td>Yes</td>
<td>No</td>
<td>See DCERPC Inspection, page 11-1.</td>
</tr>
<tr>
<td>DNS</td>
<td>Yes</td>
<td>Yes</td>
<td>See DNS Inspection, page 8-1.</td>
</tr>
<tr>
<td>ESMTP</td>
<td>Yes</td>
<td>No</td>
<td>See SMTP and Extended SMTP Inspection, page 8-32.</td>
</tr>
<tr>
<td>FTP</td>
<td>Yes</td>
<td>Yes</td>
<td>See FTP Inspection, page 8-7.</td>
</tr>
<tr>
<td>GTP</td>
<td>Yes</td>
<td>No</td>
<td>See GTP Inspection, page 11-4.</td>
</tr>
<tr>
<td>H.323 RAS</td>
<td>Yes</td>
<td>Yes</td>
<td>See H.323 Inspection, page 9-2.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Yes</td>
<td>Yes</td>
<td>See HTTP Inspection, page 8-13.</td>
</tr>
</tbody>
</table>
### Table 7-2 Inspection Protocols (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supports Inspection Policy Maps</th>
<th>Supports Inspection Class Maps</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>No</td>
<td>No</td>
<td>See ICMP Inspection, page 8-19.</td>
</tr>
<tr>
<td>ICMP Error</td>
<td>No</td>
<td>No</td>
<td>See ICMP Error Inspection, page 8-19.</td>
</tr>
<tr>
<td>ILS</td>
<td>No</td>
<td>No</td>
<td>See ILS Inspection, page 10-1.</td>
</tr>
<tr>
<td>IM</td>
<td>Yes</td>
<td>Yes</td>
<td>See Instant Messaging Inspection, page 8-19.</td>
</tr>
<tr>
<td>IP-Options</td>
<td>Yes</td>
<td>No</td>
<td>See IP Option Inspection, page 8-22.</td>
</tr>
<tr>
<td>MGCP</td>
<td>Yes</td>
<td>No</td>
<td>See MGCP Inspection, page 9-9.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Yes</td>
<td>No</td>
<td>See NetBIOS Inspection, page 8-30.</td>
</tr>
<tr>
<td>PPTP</td>
<td>No</td>
<td>No</td>
<td>See PPTP Inspection, page 8-31.</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>Yes</td>
<td>No</td>
<td>See RADIUS Accounting Inspection, page 11-8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RADIUS accounting inspection is available for a management service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>policy only. You must select a policy map to implement this inspection.</td>
</tr>
<tr>
<td>RSH</td>
<td>No</td>
<td>No</td>
<td>See RSH Inspection, page 11-11.</td>
</tr>
<tr>
<td>RTSP</td>
<td>Yes</td>
<td>No</td>
<td>See RTSP Inspection, page 9-12.</td>
</tr>
<tr>
<td>SIP</td>
<td>Yes</td>
<td>Yes</td>
<td>See SIP Inspection, page 9-17.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td>No</td>
<td>See SNMP Inspection, page 11-11.</td>
</tr>
<tr>
<td>SQLNET</td>
<td>No</td>
<td>No</td>
<td>See SQL*Net Inspection, page 10-2.</td>
</tr>
<tr>
<td>SUNRPC</td>
<td>No</td>
<td>No</td>
<td>See Sun RPC Inspection, page 10-3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default class map includes UDP port 111; if you want to enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sun RPC inspection for TCP port 111, you need to create a new class</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>map that matches TCP port 111, add the class to the policy, and then</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>apply the inspect sunrpc command to that class.</td>
</tr>
<tr>
<td>TFTP</td>
<td>No</td>
<td>No</td>
<td>See TFTP Inspection, page 8-37.</td>
</tr>
<tr>
<td>WAAS</td>
<td>No</td>
<td>No</td>
<td>Enables TCP option 33 parsing. Use when deploying Cisco Wide Area</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application Services products.</td>
</tr>
<tr>
<td>XDMCP</td>
<td>No</td>
<td>No</td>
<td>See XDMCP Inspection, page 11-12.</td>
</tr>
</tbody>
</table>

**Step 6** You can configure other features for this rule if desired using the other Rule Actions tabs.

**Step 7** Click **OK** (or **Finish** from the wizard).
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, page 7-11
- Create a Regular Expression Class Map, page 7-14

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

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>(exp)</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(ola)g matches dog and dag, but dolag matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, ab(xy){3}z matches abxyxyxxyz.</td>
</tr>
<tr>
<td></td>
<td>Alternation</td>
<td>Matches either expression it separates. For example, doglcat matches dog or cat.</td>
</tr>
<tr>
<td>?</td>
<td>Question mark</td>
<td>A quantifier that indicates that there are 0 or 1 of the previous expression. For example, lo?se matches lse or lose.</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, lo*se matches lse, lose, loose, and so on.</td>
</tr>
</tbody>
</table>
Configure Regular Expressions

Step 1  Choose Configuration > Firewall > Objects > Regular Expressions.

Step 2  In the Regular Expressions area, do one of the following:

- Choose Add to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click Edit.

---

### Table 7-3  Regular Expression Metacharacters (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Plus</td>
<td>A quantifier that indicates that there is at least 1 of the previous expression. For example, \bse matches lose and loose, but not lse.</td>
</tr>
<tr>
<td>{x} or {x,}</td>
<td>Minimum repeat quantifier</td>
<td>Repeat at least x times. For example, \bxyz matches abxyxyz, abxyxyxyz, and so on.</td>
</tr>
<tr>
<td>[abc]</td>
<td>Character class</td>
<td>Matches any character in the brackets. For example, \abc matches a, b, or c.</td>
</tr>
<tr>
<td>[^abc]</td>
<td>Negated character class</td>
<td>Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than a, b, or c. [^[A-Z] matches any single character that is not an uppercase letter.</td>
</tr>
<tr>
<td>[a-c]</td>
<td>Character range class</td>
<td>Matches any character in the range. [a-z] matches any lowercase letter. You can mix characters and ranges: [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z]. The dash (-) character is literal only if it is the last or the first character within the brackets: [abc-] or [a-c] and so does [a-c].</td>
</tr>
<tr>
<td>&quot;</td>
<td>Quotation marks</td>
<td>Preserves trailing or leading spaces in the string. For example, “test” preserves the leading space when it looks for a match.</td>
</tr>
<tr>
<td>^</td>
<td>Caret</td>
<td>Specifies the beginning of a line.</td>
</tr>
<tr>
<td>\</td>
<td>Escape character</td>
<td>When used with a metacharacter, matches a literal character. For example, [ matches the left square bracket.</td>
</tr>
<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>
Step 3  Either enter the regular expression in the Value field, or click Build to get help creating the expression. The regular expression is limited to 100 characters in length.

If you click Build, use the following process to create the expression:

a. In the Build Snippet area, create a component of the expression using the following options. Look at the Snippet Preview area at the end of this section to see the expression you are building.

   - Starts at the beginning of the line (^)—Indicates that the snippet should start at the beginning of a line, using the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
   - Specify Character String—If you are trying to match a specific string, such as a word or phrase, enter the string.
     If there are any metacharacters in your text string that you want to be used literally, choose Escape Special Characters to add the backslash (\) escape character before them. For example, if you enter “example.com,” this option converts it to “example\.com”.
     If you want to match upper and lower case characters, choose Ignore Case. For example, “cats” is converted to “[cC][aA][rT][sS]”.
   - Specify Character—If you are trying to match a specific type of character or set of characters, rather than a particular phrase, select this option and identify the characters using these options:
     Negate the character—Specifies not to match the character you identify.
     Any character (.)—Inserts the period (.) metacharacter to match any character. For example, d.g matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
     Character set—Inserts a character set. Text can match any character in the set. For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (upper or lower case) or any digit 0 through 9. The \[\n\f\r\t\] set matches a new line, form feed, carriage return, or a tab.
     Special character—Inserts a character that requires an escape, including \, ?, *, +, |, ., [ ], ( ), or ^.
     Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
     Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
     Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
     Specified character—Enter any single character.
   b. Add the snippet to the regular expression box using one of the following buttons. Note that you can also type directly in the regular expression.
      - Append Snippet—Adds the snippet to the end of the regular expression.
      - Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, dog|cat matches dog or cat.
      - Insert Snippet at Cursor—Inserts the snippet at the cursor.
   c. Repeat the process to add snippets until the expression is complete.
Configure Regular Expressions

Chapter 7  Getting Started with Application Layer Protocol Inspection

Configure Regular Expressions

- (Optional.) In Selection Occurrences, select how often the expression or parts of it must match text to be considered a match. Select text in the Regular Expression field, click one of the following options, and then click Apply to Selection. For example, if the regular expression is “test me,” and you select “me” and apply One or more times, then the regular expression changes to “test (me)+”.
  - Zero or one times (?)—There are 0 or 1 of the previous expression. For example, lo?se matches lse or lose.
  - One or more times (+)—There is at least 1 of the previous expression. For example, lo+se matches lose and loose, but not lse.
  - Any number of times (*)—There are 0, 1 or any number of the previous expression. For example, lo*se matches lse, lose, loose, and so on.
  - At least—Repeat at least x times. For example, ab(xy){2,}z matches abxyxyz, abxyxyxyz, and so on.
  - Exactly—Repeat exactly x times. For example, ab(xy){3}z matches abxyxyz.

- Click Test to verify your expression will match the intended text. If the test is unsuccessful, you can try editing it in the test dialog, or return to the expression builder. If you edit the expression in the text dialog and click OK, the edits are saved and reflected in the expression builder.

- Click OK.

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  Choose Configuration > Firewall > Objects > Regular Expressions.

Step 2  In the Regular Expressions Classes area, do one of the following:
  - Choose Add to add a new class map. Enter a name and optionally, a description.
  - Choose an existing class map and click Edit.

Step 3  Select the expressions you want in the map and click Add. Remove any you do not want.

Step 4  Click OK.
## 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, regex, match regex</code>.</td>
</tr>
<tr>
<td>Match any for inspection policy maps</td>
<td>8.0(2)</td>
<td>The <code>match any</code> keyword was introduced for use with inspection policy maps: traffic can match one or more criteria to match the class map. Formerly, only <code>match all</code> 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, page 7-1.

- DNS Inspection, page 8-1
- FTP Inspection, page 8-7
- HTTP Inspection, page 8-13
- ICMP Inspection, page 8-19
- ICMP Error Inspection, page 8-19
- Instant Messaging Inspection, page 8-19
- IP Options Inspection, page 8-22
- IPsec Pass Through Inspection, page 8-25
- IPv6 Inspection, page 8-28
- NetBIOS Inspection, page 8-30
- PPTP Inspection, page 8-31
- SMTP and Extended SMTP Inspection, page 8-32
- TFTP Inspection, page 8-37

DNS Inspection

The following sections describe DNS application inspection.

- DNS Inspection Actions, page 8-2
- Defaults for DNS Inspection, page 8-2
- Configure DNS Inspection, page 8-2
- Monitoring DNS Inspection, page 8-7
DNS Inspection Actions

DNS inspection is enabled by default. You can customize DNS inspection to perform many tasks:

- Translate the DNS record based on the NAT configuration. For more information, see DNS and NAT, page 6-39.
- Enforce message length, domain-name length, and label length.
- Verify the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message.
- Check to see if a compression pointer loop exists.
- Inspect packets based on the DNS header, type, class and more.

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.
- 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.

Configure DNS Inspection

DNS inspection is enabled by default. You need to configure it only if you want non-default processing. If you want to customize DNS inspection, use the following process.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure DNS Inspection Class Map, page 8-2.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure DNS Inspection Policy Map, page 8-4.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the DNS Inspection Service Policy, page 8-6.</td>
</tr>
</tbody>
</table>

Configure DNS Inspection Class Map

You can optionally create a DNS inspection class map to define the traffic class for DNS inspection. The other option is to define the traffic classes directly in the DNS inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.
Tip
You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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** Choose Configuration > Firewall > Objects > Class Maps > DNS.

**Step 2** Do one of the following:
- Click Add to add a new class map.
- Select a map and click Edit.

**Step 3** For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

**Step 4** Choose a match option: Match All or Match Any.

**Match All** is the default, and specifies that traffic must match all criteria to match the class map. **Match Any** means that traffic matches the class map if it matches at least one criterion.

**Step 5** Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: Match (traffic must match the criterion) or No Match (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

b. Choose the match criterion and define its value:
- Header Flag—Select whether the flag should equal or contain the specified value, then either select the header flag name, or enter the hex value of the header (0x0 to 0xffff). If you select multiple header values, “equals” requires that all flags are present, “contains” that any one of the flags is present, in the packet. Header flag names are AA (Authoritative Answer), QR (Query), RA (Recursion Available), RD (Recursion Desired), TC (Truncation).
- Type—The DNS Type field name or value in the packet. Field names are A (IPv4 address), AXFR (full zone transfer), CNAME (canonical name), IXFR (incremental zone transfer), NS (authoritative name server), SOA (start of a zone of authority) or TSIG (transaction signature). Values are arbitrary numbers in the DNS Type field from 0 to 65535: either enter a specific value or a range of values.
- Class—The DNS Class field name or value in the packet. Internet is the only possible field name. Values are arbitrary numbers in the DNS Class field from 0 to 65535: either enter a specific value or a range of values.
- Question—The question portion of a DNS message.
- Resource Record—The DNS resource record. Choose whether to match the additional, answer, or authority resource record section.

c. Click OK.

**Step 6** Click OK in the DNS Traffic Class Map dialog box.
You can now use the class map in a DNS inspection policy map.

### 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.

**Tip**
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

**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** Choose Configuration > Firewall > Objects > Inspect Maps > DNS.

**Step 2** Do one of the following:
- Click **Add** to add a new map.
- Select a map to view its contents. You can change the security level directly, or click **Customize** to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

**Step 3** For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

**Step 4** In the **Security Level** view of the DNS Inspect Map dialog box, select the level that best matches your desired configuration. The default level is Low.

If one of the preset levels matches your requirements, you are now done. Just click **OK**, skip the rest of this procedure, and use the map in a service policy rule for DNS inspection.

If you need to customize the settings further, click **Details**, and continue with the procedure.

**Step 5** Click the **Protocol Conformance** tab and choose the desired options:
- **Enable DNS guard function**—Using 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.
- **Enable NAT re-write function**—Translates the DNS record based on the NAT configuration.
- **Enable 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.
- **Randomize the DNS identifier for DNS query**.
- **Enforce TSIG resource record to be present in DNS message**—You can drop or log non-conforming packets, and optionally log dropped packets.

**Step 6** Click the **Filtering** tab and choose the desired options.
- **Global Settings**—Choose whether to drop packets that exceed the specified maximum length regardless of whether they are from the client or server, from 512 to 65535 bytes.
Chapter 8  Inspection of Basic Internet Protocols

DNS Inspection

- **Server Settings**—*Drop packets that exceed specified maximum length* and *Drop packets sent to server that exceed length indicated by the RR*—Sets the maximum server DNS message length, from 512 to 65535 bytes, or sets the maximum length to the value in the Resource Record. If you enable both settings, the lower value is used.

- **Client Settings**—*Drop packets that exceed specified maximum length* and *Drop packets sent to server that exceed length indicated by the RR*—Sets the maximum client DNS message length, from 512 to 65535 bytes, or sets the maximum length to the value in the Resource Record. If you enable both settings, the lower value is used.

**Step 7** Click the **Mismatch Rate** tab and choose whether to enable logging when the DNS ID mismatch rate exceeds the specified threshold. For example, you could set a threshold of 30 mismatches per 3 seconds.

**Step 8** Click the **Inspections** tab and define the specific inspections you want to implement based on traffic characteristics.

You can define traffic matching criteria based on DNS class maps, by configuring matches directly in the inspection map, or both.

a. Do any of the following:
   - Click **Add** to add a new criterion.
   - Select an existing criterion and click **Edit**.

b. Choose **Single Match** to define the criterion directly, or **Multiple Match**, in which case you select the DNS class map that defines the criteria (see Configure DNS Inspection Class Map, page 8-2.)

c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map. Then, configure the criterion as follows:
   - **Header Flag**—Select whether the flag should equal or contain the specified value, then either select the header flag name, or enter the hex value of the header (0x0 to 0xffff). If you select multiple header values, “equals” requires that all flags are present, “contains” that any one of the flags is present, in the packet. Header flag names are **AA** (Authoritative Answer), **QR** (Query), **RA** (Recursion Available), **RD** (Recursion Desired), **TC** (Truncation).
   - **Type**—The DNS Type field name or value in the packet. Field names are **A** (IPv4 address), **AXFR** (full zone transfer), **CNAME** (canonical name), **IXFR** (incremental zone transfer), **NS** (authoritative name server), **SOA** (start of a zone of authority) or **TSIG** (transaction signature). Values are arbitrary numbers in the DNS Type field from 0 to 65535: either enter a specific value or a range of values.
   - **Class**—The DNS Class field name or value in the packet. Internet is the only possible field name. Values are arbitrary numbers in the DNS Class field from 0 to 65535: either enter a specific value or a range of values.
   - **Question**—The question portion of a DNS message.
   - **Resource Record**—The DNS resource record. Choose whether to match the additional, answer, or authority resource record section.

d. Choose the primary action to take for matching traffic: drop packet, drop connection, mask (for Header Flag matches only) or none.

e. Choose whether to enable or disable logging. You must disable logging if you want to enforce TSIG.

f. Choose whether to enforce the presence of a TSIG resource record. You can drop the packet, log it, or drop and log it. Usually, you must select **Primary Action: None** and **Log: Disable** to enforce TSIG. However, for Header Flag matches, you can enforce TSIG along with the mask primary action.
g. Click OK to add the inspection. Repeat the process as needed.

**Step 9**

Click OK in the DNS Inspect Map dialog box.

You can now use the inspection map in a DNS inspection service policy.

---

**Configure the DNS Inspection Service Policy**

The default ASA configuration includes DNS inspection on the default port applied globally on all interfaces. 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.

**Procedure**

**Step 1**

Choose Configuration > Firewall > Service Policy, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.
- To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have a DNS inspection rule, or a rule to which you are adding DNS inspection, select it and click Edit.

**Step 2**

On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

**Step 3**

(To change an in-use policy) If you are editing any in-use policy to use a different DNS inspection policy map, you must disable the DNS inspection, and then re-enable it with the new DNS inspection policy map name:

a. Uncheck the DNS check box.

b. Click OK.

c. Click Apply.

d. Repeat these steps to return to the Protocol Inspections tab.

**Step 4**

Select DNS.

**Step 5**

If you want non-default inspection, click Configure and do the following:

a. Choose whether to use the default map or to use a DNS inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure DNS Inspection Policy Map, page 8-4.

b. If you are using the Botnet Traffic Filter, choose Enable DNS snooping. 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. If you want to inspect encrypted SIP traffic, choose Enable encrypted traffic inspection and select a TLS proxy (click Manage to create one if necessary). For example, if the DNS server is on the outside interface, you should enable DNS inspection with snooping for all UDP DNS traffic on the outside interface.

c. Click OK in the Select DNS Inspect Map dialog box.
Monitoring DNS Inspection

To view information about the current DNS connections, enter the following command in Tools > Command Line Interface or use Monitoring > Properties > Connections:

```
hostname# show conn
```

For connections using a DNS server, the source port of the connection may be replaced by the IP address of the DNS server in the show conn command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by app_id, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, when you enter the `show conn` command, you see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

To display the statistics for DNS application inspection, enter the `show service-policy` command. The following is sample output from the `show service-policy` command:

```
hostname# show service-policy
Interface outside:
  Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP Inspection

The following sections describe the FTP inspection engine.

- FTP Inspection Overview, page 8-7
- Strict FTP, page 8-8
- Configure FTP Inspection, page 8-9
- Verifying and Monitoring FTP Inspection, page 8-13

FTP Inspection Overview

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address
FTP application inspection prepares secondary channels for FTP data transfer. Ports for these channels are negotiated through PORT or PASV commands. The channels are allocated in response to a file upload, a file download, or a directory listing event.

**Note**

If you disable FTP inspection engines with the `no inspect ftp` command, 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, click the **Configure** button next to FTP on the Configuration > Firewall > Service Policy Rules > Edit Service Policy Rule > Rule Actions > Protocol Inspection tab.

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.

After you enable the **strict** option on an interface, 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 the **strict** option may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

If the **strict** option is enabled, each FTP command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the PORT and PASV reply command is checked to see if it is five. If it is not five, then the PORT command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the FTP command to see if it ends with `<CR><LF>` characters, as required by the RFC. If it does not, the connection is closed.
- Size of RETR and STOR commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The PORT command should always be sent from the client. The TCP connection is denied if a PORT command is sent from the server.
- Reply spoofing—PASV reply command (227) should always be sent from the server. The TCP connection is denied if a PASV reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing—The 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 FTP Inspection

FTP inspection is enabled by default. You need to configure it only if you want non-default processing. If you want to customize FTP inspection, use the following process.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure FTP Inspection Class Map, page 8-9.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure an FTP Inspection Policy Map, page 8-10.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the FTP Inspection Service Policy, page 8-12.</td>
</tr>
</tbody>
</table>

### Configure FTP Inspection Class Map

You can optionally create an FTP inspection class map to define the traffic class for FTP inspection. The other option is to define the traffic classes directly in the FTP inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.

**Tip**

You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

**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</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Firewall &gt; Objects &gt; Class Maps &gt; FTP.</td>
</tr>
</tbody>
</table>
| Step 2 | Do one of the following:  
  • Click Add to add a new class map.  
  • Select a map and click Edit. |
| Step 3 | For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only. |
| Step 4 | Choose a match option: **Match All** or **Match Any**.  
**Match All** is the default, and specifies that traffic must match all criteria to match the class map. **Match Any** means that traffic matches the class map if it matches at least one criterion. |
Step 5 Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

b. Choose the match criterion and define its value:
   - File Name—Match the name of the file being transferred against the selected regular expression or regular expression class.
   - File Type—Match the MIME or media type of the file being transferred against the selected regular expression or regular expression class.
   - Server—Match the FTP server name against the selected regular expression or regular expression class.
   - User—Match the name of the logged-in user against the selected regular expression or regular expression class.
   - Request Command—The FTP command used in the packet, any combination 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.
     - 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.

c. Click **OK**.

Step 6 Click **OK** in the FTP Traffic Class Map dialog box.

You can now use the class map in an FTP inspection policy 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.

Tip
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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 Choose Configuration > Firewall > Objects > Inspect Maps > FTP.
Step 2 Do one of the following:
- Click Add to add a new map.
- Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.
Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4 In the Security Level view of the FTP Inspect Map dialog box, select the level that best matches your desired configuration. The default level is High.
   If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for FTP inspection.
   If you need to customize the settings further, click Details, and continue with the procedure.

Tip
The File Type Filtering button is a shortcut to configure file media or MIME type inspection, which is explained later in this procedure.

Step 5 Click the Parameters tab and choose whether to mask the greeting banner from the server or mask the reply to the SYST command.
   Masking these items prevents the client from discovering server information that might be helpful in an attack.
Step 6 Click the Inspections tab and define the specific inspections you want to implement based on traffic characteristics.
   You can define traffic matching criteria based on FTP class maps, by configuring matches directly in the inspection map, or both.
   a. Do any of the following:
      - Click Add to add a new criterion.
      - Select an existing criterion and click Edit.
   b. Choose Single Match to define the criterion directly, or Multiple Match, in which case you select the FTP class map that defines the criteria (see Configure FTP Inspection Class Map, page 8-9.)
FTP Inspection

Chapter 8      Inspection of Basic Internet Protocols

c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the class map. Then, configure the criterion as described in Configure FTP Inspection Class Map, page 8-9.

d. Choose whether to enable or disable logging. The action is always to reset the connection, which drops the packet, closes the connection, and sends a TCP reset to the server or client.

e. Click **OK** to add the inspection. Repeat the process as needed.

**Step 7** Click **OK** in the FTP Inspect Map dialog box.

You can now use the inspection map in a FTP inspection service policy.

---

**Configure the FTP Inspection Service Policy**

The default ASA configuration includes FTP inspection on the default port applied globally on all interfaces. 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.

**Procedure**

**Step 1** Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have a FTP inspection rule, or a rule to which you are adding FTP inspection, select it and click **Edit**.

**Step 2** On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3** (To change an in-use policy) If you are editing any in-use policy to use a different FTP inspection policy map, you must disable the FTP inspection, and then re-enable it with the new FTP inspection policy map name:

- Uncheck the **FTP** check box.
- Click **OK**.
- Click **Apply**.
- Repeat these steps to return to the Protocol Inspections tab.

**Step 4** Select **FTP**.

**Step 5** If you want non-default inspection, click **Configure**, and do the following:

- Select **Use Strict FTP**.
- Choose whether to use the default map or to use a FTP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure an FTP Inspection Policy Map, page 8-10.
- Click **OK** in the Select FTP Inspect Map dialog box.
Step 6  Click **OK** or **Finish** to save the service policy rule.

---

**Verifying and Monitoring FTP Inspection**

FTP application inspection generates the following log messages:

- An Audit record 303002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

---

**HTTP Inspection**

The following sections describe the HTTP inspection engine.

- **HTTP Inspection Overview, page 8-13**
- **Configure HTTP Inspection, page 8-14**

---

**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 HTTP Inspection

HTTP inspection is not enabled by default. 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 using the following process.

### Tip

Do not configure HTTP inspection in both a service module and on the ASA, as the inspections are not compatible.

### Procedure

**Step 1** Configure HTTP Inspection Class Map, page 8-14.

**Step 2** Configure an HTTP Inspection Policy Map, page 8-16.

**Step 3** Configure the HTTP Inspection Service Policy, page 8-18.

## Configure HTTP Inspection Class Map

You can optionally create an HTTP inspection class map to define the traffic class for HTTP inspection. The other option is to define the traffic classes directly in the HTTP inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.

### Tip

You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

**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** Choose Configuration > Firewall > Objects > Class Maps > HTTP.

**Step 2** Do one of the following:
Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 Choose a match option: **Match All** or **Match Any**.

**Match All** is the default, and specifies that traffic must match all criteria to match the class map. **Match Any** means that traffic matches the class map if it matches at least one criterion.

Step 5 Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

b. Choose the match criterion and define its value:

- Request/Response Content Type Mismatch—Match packets where the content type in the response does not match one of the MIME types in the accept field of the request.
- Request Arguments—Match the arguments of the request against the selected regular expression or regular expression class.
- Request Body Length—Match packets where the body of the request is greater than the specified number of bytes.
- Request Body—Match the body of the request against the selected regular expression or regular expression class.
- Request Header Field Count—Match packets where the number of header fields in the request is greater than the specified count. You can match the field header type to a regular expression or to a predefined type. The predefined types 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.
- Request Header Field Length—Match packets where the length of the header field in the request is greater than the specified bytes. You can match the field header type to a regular expression or to a predefined type. The predefined types are listed above for Request Header Field Count.
- Request Header Field—Match the content of the selected header field in the request against the selected regular expression or regular expression class. You can specify a predefined header type or use a regular expression to select the headers.
- Request Header Count—Match packets where the number of headers in the request is greater than the specified number.
- Request Header Length—Match packets where the length of the header in the request is greater than the specified bytes.
- Request Header Non-ASCII—Match packets where the header in the request contains non-ASCII characters.
- Request Method—Match packets where the request method matches the predefined type or the selected regular expression or regular expression class. The predefined types are: bcopy, bdelete, bmove, bpropfind, bpropatch, connect, copy, delete, edit, get, getattribute,
Chapter 8  Inspection of Basic Internet Protocols

HTTP Inspection

getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, remlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.

- Request URI Length—Match packets where the length of the URI of the request is greater than the specified bytes.
- Request URI—Match the content of the URI of the request against the selected regular expression or regular expression class.
- Request Body—Match the body of the request against the selected regular expression or regular expression class, or to ActiveX or Java Applet content.
- Response Body Length—Match packets where the length of the body of the response is greater than the specified bytes.
- Response Header Field Count—Match packets where the number of header fields in the response is greater than the specified count. You can match the field header type to a regular expression or to a predefined type. The predefined types 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.
- Response Header Field Length—Match packets where the length of the header field in the response is greater than the specified bytes. You can match the field header type to a regular expression or to a predefined type. The predefined types are listed above for Response Header Field Count.
- Response Header Field—Match the content of the selected header field in the response against the selected regular expression or regular expression class. You can specify a predefined header type or use a regular expression to select the headers.
- Response Header Count—Match packets where the number of headers in the response is greater than the specified number.
- Response Header Length—Match packets where the length of the header in the response is greater than the specified bytes.
- Response Header Non-ASCII—Match packets where the header in the response contains non-ASCII characters.
- Response Status Line—Match the content of the response status line against the selected regular expression or regular expression class.

c.  Click OK.

Step 6  Click OK in the HTTP Traffic Class Map dialog box.
You can now use the class map in an HTTP inspection policy map.

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.

Tip
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.
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 Choose Configuration > Firewall > Objects > Inspect Maps > HTTP.

Step 2 Do one of the following:

- Click Add to add a new map.
- Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 In the Security Level view of the HTTP Inspect Map dialog box, select the level that best matches your desired configuration. The default level is Low.

If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for HTTP inspection.

If you need to customize the settings further, click Details, and continue with the procedure.

Tip The URI Filtering button is a shortcut to configure Request URI inspection, which is explained later in this procedure.

Step 5 Click the Parameters tab and configure the desired options.

- **Body Match Maximum**—The maximum number of characters in the body of an HTTP message that should be searched in a body match. Default is 200 bytes. A large number will have a significant impact on performance.

- **Check for protocol violations**—Whether to verify that packets conform to the HTTP protocol. For violations, you can drop the connection, reset it, or log it. When dropping or resetting, you can also enable logging.

- **Spoof server string**—Replaces the server HTTP header value with the specified string, up to 82 characters.

Step 6 Click the Inspections tab and define the specific inspections you want to implement based on traffic characteristics.

You can define traffic matching criteria based on HTTP class maps, by configuring matches directly in the inspection map, or both.

a. Do any of the following:

- Click Add to add a new criterion.
- Select an existing criterion and click Edit.

b. Choose **Single Match** to define the criterion directly, or **Multiple Match**, in which case you select the HTTP class map that defines the criteria (see Configure HTTP Inspection Class Map, page 8-14.)

c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded.
HTTP Inspection

from the class map. Then, configure the criterion as described in Configure HTTP Inspection Class Map, page 8-14.

d. Choose whether to drop the connection, reset it, or log it. For drop connection and reset, you can enable or disable logging.

e. Click OK to add the inspection. Repeat the process as needed.

Step 7 Click OK in the HTTP Inspect Map dialog box.

You can now use the inspection map in a HTTP inspection service policy.

Configure the HTTP Inspection Service Policy

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.

Procedure

Step 1 Choose Configuration > Firewall > Service Policy, and open a rule.

• To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.

• To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.

• If you have an HTTP inspection rule, or a rule to which you are adding HTTP inspection, select it and click Edit.

Step 2 On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

Step 3 (To change an in-use policy) If you are editing any in-use policy to use a different HTTP inspection policy map, you must disable the HTTP inspection, and then re-enable it with the new HTTP inspection policy map name:

a. Uncheck the HTTP check box.

b. Click OK.

c. Click Apply.

d. Repeat these steps to return to the Protocol Inspections tab.

Step 4 Select HTTP.

Step 5 If you want non-default inspection, click Configure, and do the following:

a. Choose whether to use the default map or to use an HTTP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure an HTTP Inspection Policy Map, page 8-16.

b. Click OK in the Select HTTP Inspect Map dialog box.

Step 6 Click OK or Finish to save the service policy rule.
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, page 7-8.

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.

The ICMP payload is scanned to retrieve the five-tuple from the original packet. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. The ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the mapped IP is changed to the real IP (Destination Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet mapped IP is changed to the real IP
  - Original packet mapped port is changed to the real Port
  - Original packet IP checksum is recalculated

For information on enabling ICMP Error inspection, see Configure Application Layer Protocol Inspection, page 7-8.

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 by default. You must configure it if you want IM inspection.
Instant Messaging Inspection

Chapter 8      Inspection of Basic Internet Protocols

Configure an Instant Messaging Inspection Policy Map

To specify actions when a message violates a parameter, create an IM inspection policy map. You can then apply the inspection policy map when you enable IM inspection.

You can optionally create an IM inspection class map to define the traffic class for IM inspection. The other option is to define the traffic classes directly in the IM inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps. This procedure explains inspection maps, but class maps are essentially the same, except that you do not specify the actions for matching traffic. You can configure IM class maps by selecting Configuration > Firewall > Objects > Class Maps > Instant Messaging (IM).

Tip

You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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 Configure an Instant Messaging Inspection Policy Map, page 8-20.
Step 2 Configure the IM Inspection Service Policy, page 8-21.

Configure an Instant Messaging Inspection Policy Map

To specify actions when a message violates a parameter, create an IM inspection policy map. You can then apply the inspection policy map when you enable IM inspection.

You can optionally create an IM inspection class map to define the traffic class for IM inspection. The other option is to define the traffic classes directly in the IM inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps. This procedure explains inspection maps, but class maps are essentially the same, except that you do not specify the actions for matching traffic. You can configure IM class maps by selecting Configuration > Firewall > Objects > Class Maps > Instant Messaging (IM).

Tip

You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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 Choose Configuration > Firewall > Objects > Inspect Maps > Instant Messaging (IM).
Step 2 Do one of the following:
   - Click Add to add a new map.
   - Select a map and click Edit.
Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4 Define the specific inspections you want to implement based on traffic characteristics.
You can define traffic matching criteria based on IM class maps, by configuring matches directly in the inspection map, or both.
   a. Do any of the following:
      - Click Add to add a new criterion.
      - Select an existing criterion and click Edit.
   b. Choose Single Match to define the criterion directly, or Multiple Match, in which case you select the IM class map that defines the criteria. Click Manage to create new class maps.
c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map. Then, configure the criterion.

- **Protocol**—Match traffic of a specific IM protocol, such as Yahoo Messenger or MSN Messenger.
- **Service**—Match a specific IM service, such as chat, file transfer, web cam, voice chat, conference, or games.
- **Version**—Match the version of the IM message against the selected regular expression or regular expression class.
- **Client Login Name**—Match the source client login name of the IM message against the selected regular expression or regular expression class.
- **Client Peer Login Name**—Match the destination peer login name of the IM message against the selected regular expression or regular expression class.
- **Source IP Address**—Match the source IP address and mask.
- **Destination IP Address**—Match the destination IP address and mask.
- **Filename**—Match the filename of the IM message against the selected regular expression or regular expression class.

d. Choose whether to drop the connection, reset it, or log it. For drop connection and reset, you can enable or disable logging.

e. Click OK to add the inspection. Repeat the process as needed.

---

### Step 5

Click **OK** in the IM Inspect Map dialog box.

You can now use the inspection map in an IM inspection service policy.

---

### Configure the IM Inspection Service Policy

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.

#### Procedure

**Step 1**

Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic**, page 1-10.
- If you have an IM inspection rule, or a rule to which you are adding IM inspection, select it and click **Edit**.

**Step 2**

On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.
IP Options Inspection

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. Configuring this inspection instructs the ASA to allow a packet to pass or to clear the specified IP options and then allow the packet to pass.

The following sections describe the IP Options inspection engine.

- IP Options Inspection Overview, page 8-22
- Defaults for IP Options Inspection, page 8-23
- Configure IP Options Inspection, page 8-23
- Monitoring IP Options Inspection, page 8-25

IP Options Inspection Overview

Each IP packet contains an IP header with the Options field. The Options field, commonly referred to as IP Options, provide for 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.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. Configuring this inspection instructs the ASA to allow a packet to pass or to clear the specified IP options and then allow the packet to pass.
What Happens When You Clear an Option

When you configure an IP options inspection policy map, you can specify whether you want to allow or clear each option type. If you do not specify an option type, packets that contain the option are dropped.

If you simply allow an option, packets containing the option are passed through unchanged.

If you specify that you want to clear an option from IP headers, the IP header changes in the following ways:

- The option is removed from the header.
- The Options field is padded so that the field ends on a 32 bit boundary.
- Internet header length (IHL) in the packet changes.
- The total length of the packet changes.
- The checksum is recomputed.

Supported IP Options for Inspection

IP Options inspection can check for the following IP options in a packet. If an IP header contains additional options other than these, regardless of whether the ASA is configured to allow these options, the ASA will drop the packet.

- End of Options List (EOOL) or IP Option 0—This option, which contains just a single zero byte, appears at the end of all options to mark the end of a list of options. This might not coincide with the end of the header according to the header length.

- No Operation (NOP) or IP Option 1—The Options field in the IP header can contain zero, one, or more options, which makes the total length of the field variable. However, the IP header must be a multiple of 32 bits. If the number of bits of all options is not a multiple of 32 bits, the NOP option is used as “internal padding” to align the options on a 32-bit boundary.

- Router Alert (RTRALT) or IP Option 20—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 require relatively complex processing from the routers along the packet’s delivery path. Dropping RSVP packets containing the Router Alert option can cause problems in VoIP implementations.

Defaults for IP Options Inspection

IP Options inspection is enabled by default, using the _default_ip_options_map inspection policy map.

- The Router Alert option is allowed.
- Packets that contain any other options are dropped. This includes packets that contain unsupported options.

Configure IP Options Inspection

IP options inspection is enabled by default. You need to configure it only if you want to allow additional options than the default map allows.
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 supported option type.

Tip
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

Configure the IP Options Inspection Service Policy

The default ASA configuration includes IP options inspection applied globally on all interfaces. 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.
To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.

If you have an IP options inspection rule, or a rule to which you are adding IP options inspection, select it and click Edit.

Step 2 On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

Step 3 (To change an in-use policy) If you are editing any in-use policy to use a different IP options inspection policy map, you must disable the IP options inspection, and then re-enable it with the new IP options inspection policy map name:
   a. Uncheck the IP Options check box.
   b. Click OK.
   c. Click Apply.
   d. Repeat these steps to return to the Protocol Inspections tab.

Step 4 Select IP Options.

Step 5 If you want non-default inspection, click Configure, and do the following:
   a. Choose whether to use the default map or to use an IP options inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure an IP Options Inspection Policy Map, page 8-24.
   b. Click OK in the Select IP Options Inspect Map dialog box.

Step 6 Click OK or Finish to save the service policy rule.

**Monitoring IP Options Inspection**

You can use these techniques to monitor the results of IP options inspection:

- Each time a packet is dropped due to inspection, syslog 106012 is issued. The message shows which option caused the drop.
- Use the `show service-policy inspect ip-options` command to view statistics for each option.

**IPsec Pass Through Inspection**

The following sections describe the IPsec Pass Through inspection engine.

- IPsec Pass Through Inspection Overview, page 8-25
- Configure IPsec Pass Through Inspection, page 8-26

**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 IPsec Pass Through Inspection

IPsec Pass Through inspection is not enabled by default. You must configure it if you want IPsec Pass Through inspection.

### Procedure


### 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.

**Tip**

You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

### Procedure

2. Do one of the following:
   - Click Add to add a new map.
   - Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.
3. For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4  In the Security Level view of the IPsec Pass Through Inspect Map dialog box, select the level that best matches your desired configuration.

  If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for IPsec Pass Through inspection.

  If you need to customize the settings further, click Details, and continue with the procedure.

Step 5  Choose whether to allow ESP and AH tunnels.

  For each protocol, you can also set the maximum number of connections allowed per client, and the idle timeout.

Step 6  Click OK.

  You can now use the inspection map in an IPsec Pass Through inspection service policy.

---

**Configure the IPsec Pass Through Inspection Service Policy**

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.

**Procedure**

Step 1  Choose Configuration > Firewall > Service Policy, and open a rule.

  - To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.

  - To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.

  - If you have an IPsec Pass Through inspection rule, or a rule to which you are adding IPsec Pass Through inspection, select it and click Edit.

Step 2  On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

Step 3  (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the IPsec Pass Through inspection, and then re-enable it with the new inspection policy map name:

  a. Uncheck the IPsec Pass Through check box.

  b. Click OK.

  c. Click Apply.

  d. Repeat these steps to return to the Protocol Inspections tab.

Step 4  Select IPsec Pass Through.

Step 5  If you want non-default inspection, click Configure, and do the following:

  a. Choose whether to use the default map or to use an IPsec Pass Through inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure an IPsec Pass Through Inspection Policy Map, page 8-26.

  b. Click OK in the Select IPsec Pass Through Inspect Map dialog box.
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.

- Defaults for IPv6 Inspection, page 8-28
- Configure IPv6 Inspection, page 8-28

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.

Configure IPv6 Inspection

IPv6 inspection is not enabled by default. You must configure it if you want IPv6 inspection.

Procedure

Step 2 Configure the IPv6 Inspection Service Policy, page 8-29.

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 Choose Configuration > Firewall > Objects > Inspect Maps > IPv6.
Step 2 Do one of the following:
  - Click Add to add a new map.
  - Select a map and click Edit.
Step 3  For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4  Click the Enforcement tab and choose whether to permit only known IPv6 extension headers or to enforce the order of IPv6 extension headers as defined in RFC 2460. Non-conforming packets are dropped and logged.

Step 5  (Optional) Click the Header Matches tab to identify traffic to drop or log based on the headers in IPv6 messages.

a. Do any of the following:
   - Click Add to add a new criterion.
   - Select an existing criterion and click Edit.

b. Choose the IPv6 extension header to match:
   - Authentication (AH) header.
   - Destination Options header.
   - Encapsulating Security Payload (ESP) header.
   - Fragment header.
   - Hop-by-Hop Options header.
   - Routing header—Specify either a single header type number or a range of numbers.
   - Header count—Specify the maximum number of extension headers you will allow without dropping or logging the packet.
   - Routing header address count—Specify the maximum number of addresses in the type 0 routing header you will allow without dropping or logging the packet.

c. Choose whether to drop or log the packet. If you drop the packet, you can also enable logging.

d. Click OK to add the inspection. Repeat the process as needed.

Step 6  Click OK in the IPv6 Inspect Map dialog box.

You can now use the inspection map in an IPv6 inspection service policy.

Configure the IPv6 Inspection Service Policy

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.

Procedure

Step 1  Choose Configuration > Firewall > Service Policy, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.
- To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have an IPv6 inspection rule, or a rule to which you are adding IPv6 inspection, select it and click Edit.
**Step 2** On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3** (To change an in-use policy) If you are editing any in-use policy to use a different IPv6 inspection policy map, you must disable the IPv6 inspection, and then re-enable it with the new IPv6 inspection policy map name:
   a. Uncheck the **IPv6** check box.
   b. Click **OK**.
   c. Click **Apply**.
   d. Repeat these steps to return to the Protocol Inspections tab.

**Step 4** Select **IPv6**.

**Step 5** If you want non-default inspection, click **Configure**, and do the following:
   a. Choose whether to use the default map or to use an IPv6 inspection policy map that you configured. You can create the map at this time. For detailed information, see **Configure an IPv6 Inspection Policy Map**, page 8-28.
   b. Click **OK** in the Select IPv6 Inspect Map dialog box.

**Step 6** Click **OK** or **Finish** to save the service policy rule.

---

**NetBIOS Inspection**

NetBIOS inspection is enabled by default. The NetBIOS inspection engine translates IP addresses in the NetBIOS name service (NBNS) packets according to the ASA NAT configuration. You can optionally create a policy map to drop or log NetBIOS protocol violations.

**Procedure**

**Step 1** Configure a NetBIOS Inspection Policy Map for Additional Inspection Control, page 8-30.

**Step 2** Configure the NetBIOS Inspection Service Policy, page 8-31.

---

**Configure a NetBIOS Inspection Policy Map for Additional Inspection Control**

To specify the action for protocol violations, create a NetBIOS inspection policy map. You can then apply the inspection policy map when you enable NetBIOS inspection.

**Procedure**

**Step 1** Choose **Configuration > Firewall > Objects > Inspect Maps > NetBIOS**.

**Step 2** Do one of the following:
   - Click **Add** to add a new map.
   - Select a map and click **Edit**.
Chapter 8      Inspection of Basic Internet Protocols

Step 3  For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4  Select **Check for Protocol Violations**. There is no reason to create a map if you do not select this option.

Step 5  Select the action to take, either to drop the packet or log it. If you drop the packet, you can also enable logging.

Step 6  Click **OK**.

You can now use the inspection map in a NetBIOS inspection service policy.

---

**Configure the NetBIOS Inspection Service Policy**

NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.

The default ASA configuration includes NetBIOS inspection on the default port applied globally on all interfaces. 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.

**Procedure**

**Step 1**  Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic**, page 1-10.
- If you have a NetBIOS inspection rule, or a rule to which you are adding NetBIOS inspection, select it and click **Edit**.

**Step 2**  On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3**  Select **NetBIOS**.

**Step 4**  If you want non-default inspection, click **Configure** and choose whether to use the default map or to use a NetBIOS inspection policy map that you configured. You can create the map at this time. For detailed information, see **Configure a NetBIOS Inspection Policy Map for Additional Inspection Control**, page 8-30.

**Step 5**  Click **OK** in the Select NetBIOS Inspect Map dialog box.

**Step 6**  Click **OK** or **Finish** to save the service policy rule.

---

**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 dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

For information on enabling PPTP inspection, see Configure Application Layer Protocol Inspection, page 7-8.

SMTP and Extended SMTP Inspection

ESMTP inspection detects attacks, including spam, phishing, malformed message attacks, buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detect several attacks, block senders/receivers, and block mail relay.

The following sections describe the ESMTP inspection engine.

- SMTP and ESMTP Inspection Overview, page 8-32
- Defaults for ESMTP Inspection, page 8-33
- Configure ESMTP Inspection, page 8-34

SMTP and ESMTP Inspection Overview

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. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

Extended SMTP application inspection adds support for these extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS, and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the ASA supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, ONEX, VERB, CHUNKING, and private extensions and are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: ‘XXX’.” Incomplete commands are discarded.

The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “0” characters. Carriage return (CR) and linefeed (LF) characters are ignored.
With SMTP inspection enabled, a Telnet session used for interactive SMTP may hang if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human-readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with \texttt{<CR><LR>}).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character (|) is deleted (changed to a blank space) and “<” “>” are only allowed if they are used to define a mail address (“>” must be preceded by “<”).
- Unexpected transition by the SMTP server.
- For unknown commands, the ASA changes all the characters in the packet to X. In this case, the server generates an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

### Defaults for ESMTP Inspection

ESMTP inspection is enabled by default, using the \_default\_{esmtp\_map} inspection policy map.

- The server banner is masked.
- Encrypted connections are not allowed. The STARTTLS indication is removed from the session connection attempt, forcing the client and server to negotiate a plain text session, which can be 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.
Configure ESMTP Inspection

ESMTP inspection is enabled by default. You need to configure it only if you want to different process than that provided by the default inspection map.

Procedure

Step 1  Configure an ESMTP Inspection Policy Map, page 8-34.
Step 2  Configure the ESMTP Inspection Service Policy, page 8-36.

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  Choose Configuration > Firewall > Objects > Inspect Maps > ESMTP.
Step 2  Do one of the following:
   - Click Add to add a new map.
   - Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.
Step 3  For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4  In the Security Level view of the ESMTP Inspect Map dialog box, select the level that best matches your desired configuration.

   If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for ESMTP inspection.

   If you need to customize the settings further, click Details, and continue with the procedure.

   Tip  The MIME File Type Filtering button is a shortcut to configure file type inspection, which is explained later in this procedure.

Step 5  Click the Parameters tab and configure the desired options.
   - Mask Server Banner—Whether to mask the banner from the ESMTP server.
   - Encrypted Packet Inspection—Whether to allow ESMTP over TLS (encrypted connections) without inspection. You can optionally log encrypted connections. The default is to inspect all traffic, which strips the STARTTLS indication from any encrypted session connection attempt and forces a plain-text connection.
Step 6  Click the **Filtering** tab and configure the desired options.

- **Configure mail relay**—Identifies a domain name for mail relay. You can either drop the connection and optionally log it, or log it.

- **Check for special characters**—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.

Step 7  Click the **Inspections** tab and define the specific inspections you want to implement based on traffic characteristics.

a. Do any of the following:

   - Click **Add** to add a new criterion.
   - Select an existing criterion and click **Edit**.

b. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map. Then, configure the criterion:

   - **Body Length**—Matches messages where the length of an ESMTP body message is greater than the specified number of bytes.
   - **Body Line Length**—Matches messages where the length of a line in an ESMTP body message is greater than the specified number of bytes.
   - **Commands**—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.
   - **Command Recipient Count**—Matches messages where the number of recipients is greater than the specified count.
   - **Command Line Length**—Matches messages where the length of a line in the command verb is greater than the specified number of bytes.
   - **EHLO Reply Parameters**—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.
   - **Header Length**—Matches messages where the length of an ESMTP header is greater than the specified number of bytes.
   - **Header Line Length**—Matches messages where the length of a line in an ESMTP header is greater than the specified number of bytes.
   - **Header To: Fields Count**—Matches messages where the number of To fields in the header is greater than the specified number.
   - **Invalid Recipients Count**—Matches messages where the number of invalid recipients is greater than the specified count.
   - **MIME File Type**—Matches the MIME or media file type against the specified regular expression or regular expression class.
   - **MIME Filename Length**—Matches messages where a file name is longer than the specified number of bytes.
   - **MIME Encoding**—Matches the MIME encoding type. You can specify one or more of the following types: 7bit, 8bit, base64, binary, others, quoted-printable.
• **Sender Address**—Matches the sender email address against the specified regular expression or regular expression class.

• **Sender Address Length**—Matches messages where the sender address is greater than the specified number of bytes.

c. Choose whether to drop the connection, reset it, or log it. For drop connection and reset, you can enable or disable logging. For command and EHLO reply parameter matching, you can also mask the command. For command matching, you can also apply a rate limit in packets per second.

d. Click **OK** to add the inspection. Repeat the process as needed.

**Step 8**
Click **OK** in the ESMTP Inspect Map dialog box.
You can now use the inspection map in a ESMTP inspection service policy.

---

**Configure the ESMTP Inspection Service Policy**

The default ASA configuration includes ESMTP inspection applied globally on all interfaces. 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.

**Procedure**

**Step 1**
Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have an ESMTP inspection rule, or a rule to which you are adding ESMTP inspection, select it and click **Edit**.

**Step 2**
On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3**
(To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the ESMTP inspection, and then re-enable it with the new inspection policy map name:

a. Uncheck the **ESMTP** check box.

b. Click **OK**.

c. Click **Apply**.

d. Repeat these steps to return to the Protocol Inspections tab.

**Step 4**
Select **ESMTP**.

**Step 5**
If you want non-default inspection, click **Configure**, and do the following:

a. Choose whether to use the default map or to use an ESMTP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure an ESMTP Inspection Policy Map, page 8-34.

b. Click **OK** in the Select ESMTP Inspect Map dialog box.

**Step 6**
Click **OK** or **Finish** to save the service policy rule.
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 ASA inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

For information on enabling TFTP inspection, see Configure Application Layer Protocol Inspection, page 7-8.
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, page 7-1.

- CTIQBE Inspection, page 9-1
- H.323 Inspection, page 9-2
- MGCP Inspection, page 9-9
- RTSP Inspection, page 9-12
- SIP Inspection, page 9-17
- Skinny (SCCP) Inspection, page 9-24
- History for Voice and Video Protocol Inspection, page 9-28

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, page 7-8.

- Limitations for CTIQBE Inspection, page 9-1

Limitations for CTIQBE Inspection

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations with the alias command.
- Stateful failover of CTIQBE calls is not supported.
- Debugging CTIQBE inspection might delay message transmission, which can have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the ASA, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.
The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the 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

The following sections describe the H.323 application inspection.

- H.323 Inspection Overview, page 9-2
- How H.323 Works, page 9-3
- H.239 Support in H.245 Messages, page 9-4
- Limitations for H.323 Inspection, page 9-4
- Configure H.323 Inspection, page 9-5
- Configuring H.323 and H.225 Timeout Values, page 9-8

#### H.323 Inspection Overview

H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The 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.

Note
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.

The H.323 ITU standard requires that a TPKT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as H.225 and H.245 messages, the ASA must remember the TPKT length to process and decode the messages properly. For each connection, the ASA keeps a record that contains the TPKT length for the next expected message.

If the ASA needs to perform NAT on IP addresses in messages, it changes the checksum, the UUID length, and the TPKT, if it is included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, the ASA proxy ACKs that TPKT and appends a new TPKT to the H.245 message with the new length.

Note
The ASA does not support TCP options in the Proxy ACK for the TPKT.
Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and times out with the H.323 timeout as configured in the Configuration > Firewall > Advanced > Global Timeouts pane.

**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.

**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 preformed 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:

- Only static NAT is fully supported. 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 dynamic NAT or PAT.
- Not supported with extended PAT.
- Not supported with NAT between same-security-level interfaces.
- Not supported with outside NAT.
- Not supported with NAT64.
- When a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the ASA.
- If you configure a network static address where the network static address is the same as a third-party netmask and address, then any outbound H.323 connection fails.
Configure 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. If you want to customize H.323 inspection, use the following process.

Procedure

Step 1 Configure H.323 Inspection Class Map, page 9-5
Step 2 Configure H.323 Inspection Policy Map, page 9-6
Step 3 Configure the H.323 Inspection Service Policy, page 9-8

Configure H.323 Inspection Class Map

You can optionally create an H.323 inspection class map to define the traffic class for H.323 inspection. The other option is to define the traffic classes directly in the H.323 inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.

Tip

You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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 Choose Configuration > Firewall > Objects > Class Maps > H.323.
Step 2 Do one of the following:
   - Click Add to add a new class map.
   - Select a map and click Edit.
Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4 Choose a match option: Match All or Match Any.

Match All is the default, and specifies that traffic must match all criteria to match the class map. Match Any means that traffic matches the class map if it matches at least one criterion.
Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion).

b. Choose the match criterion and define its value:
   - Called Party—Match the H.323 called party against the selected regular expression or regular expression class.
   - Calling Party—Match the H.323 calling party against the selected regular expression or regular expression class.
   - Media Type—Match the media type: audio, video, or data.

c. Click **OK**.

Step 6
Click **OK** in the H.323 Traffic Class Map dialog box.
You can now use the class map in an H.323 inspection policy map.

---

**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.

**Tip**
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

**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
Choose **Configuration > Firewall > Objects > Inspect Maps > H.323**.

Step 2
Do one of the following:
   - Click **Add** to add a new map.
   - Select a map to view its contents. You can change the security level directly, or click **Customize** to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

Step 3
For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4
In the **Security Level** view of the H.323 Inspect Map dialog box, select the level that best matches your desired configuration. The default level is Low.

If one of the preset levels matches your requirements, you are now done. Just click **OK**, skip the rest of this procedure, and use the map in a service policy rule for H.323 inspection.
Step 5 If you need to customize the settings further, click Details, and do the following:

a. Click the State Checking tab and choose whether to enable state transition checking of RAS and H.225 messages.

You can also check RCF messages and open pinholes for call signal addresses present in RRQ messages, which enables 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.

b. Click the Call Attributes tab and choose whether to enforce a call duration limit (maximum is 1193 hours) or to enforce the presence of calling and called party numbers during call setup.

c. Click the Tunneling and Protocol Conformance tab and choose whether check for H.245 tunneling; you can either drop the connection or log it.

You can also choose whether to check RTP packets that are flowing on the pinholes for protocol conformance. If you check for conformance, you can also choose whether to limit the payload to audio or video, based on the signaling exchange.

Step 6 If necessary, click the HSI Group Parameters tab and define the HSI groups.

a. Do any of the following:
   - Click Add to add a new group.
   - Select an existing group and click Edit.

b. Specify the group ID (from 0 to 2147483647) and the IP address of the HSI.

c. To add an endpoint to the HSI group, enter the IP address, select the interface through which the endpoint is connected to the ASA, and click Add>>. Remove any endpoints that are no longer needed. You can have up to 10 endpoints per group.

d. Click OK to add the group. Repeat the process as needed.

Step 7 Click the Inspections tab and define the specific inspections you want to implement based on traffic characteristics.

You can define traffic matching criteria based on H.323 class maps, by configuring matches directly in the inspection map, or both.

a. Do any of the following:
   - Click Add to add a new criterion.
   - Select an existing criterion and click Edit.

b. Choose Single Match to define the criterion directly, or Multiple Match, in which case you select the H.323 class map that defines the criteria (see Configure H.323 Inspection Class Map, page 9-5.)

c. If you are defining the criterion here, choose the match type for the criteria: Match (traffic must match the criterion) or No Match (traffic must not match the criterion). Then, configure the criterion as follows:
   - Called Party—Match the H.323 called party against the selected regular expression or regular expression class.
• Calling Party—Match the H.323 calling party against the selected regular expression or regular expression class.

• Media Type—Match the media type: audio, video, or data.

d. Choose the action to take for matching traffic. For calling or called party matching, you can drop the packet, drop the connection, or reset the connection. For media type matching, the action is always to drop the packet; you can enable logging for this action.

e. Click **OK** to add the inspection. Repeat the process as needed.

---

**Step 8**

Click **OK** in the H.323 Inspect Map dialog box.

You can now use the inspection map in an H.323 inspection service policy.

---

### Configure the H.323 Inspection Service Policy

The default ASA configuration includes H.323 H.255 and RAS inspection on the default ports applied globally on all interfaces. 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.

**Procedure**

**Step 1**

Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic, page 1-10**.
- If you have an H.323 inspection rule, or a rule to which you are adding H.323 inspection, select it and click **Edit**.

**Step 2**

On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3**

Select **H.323 H.255** and **H.323 RAS**.

**Step 4**

If you want non-default inspection, click **Configure** and choose whether to use the default map or to use an H.323 inspection policy map that you configured. You can create the map at this time. For detailed information, see **Configure H.323 Inspection Policy Map, page 9-6**.

Click **OK** in the Select H.323 Inspect Map dialog box to assign the map to the policy.

**Step 5**

Click **OK** or **Finish** to save the service policy rule.

---

### Configuring H.323 and H.225 Timeout Values

You can configure H.323/H.255 global timeout values on the **Configuration > Firewall > Advanced > Global Timeouts** page. You can set the interval for inactivity after which an H.255 signaling connection is closed (default is 1 hour) or an H.323 control connection is closed (default is 5 minutes).
MGCP Inspection

The following sections describe MGCP application inspection.

- MGCP Inspection Overview, page 9-9
- Configure MGCP Inspection, page 9-10
- Configuring MGCP Timeout Values, page 9-12

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 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 MGCP Inspection**

Use the following process to enable MGCP inspection.

**Procedure**

1. **Configuring an MGCP Inspection Policy Map for Additional Inspection Control, page 9-11.**
2. **Configure the MGCP Inspection Service Policy, page 9-11.**
Configuring an MGCP Inspection Policy Map for Additional Inspection Control

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; MGCP.</td>
</tr>
</tbody>
</table>
| Step 2 | Do one of the following:  
  - Click Add to add a new map.  
  - Select a map and click Edit. |
| Step 3 | For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only. |
| Step 4 | (Optional) Click the Command Queue tab and specify the maximum number of commands allowed in the MGCP command queue. The default is 200, the allowed range is 1 to 2147483647. |
| Step 5 | Click the Gateways and Call Agents tab and configure the groups of gateways and call agents for the map.  
  a. Click Add to create a new group, or select a group and click Edit.  
  b. Enter the Group ID of the call agent group. A call agent group associates one or more call agents with one or more MGCP media gateways. The valid range is from 0 to 2147483647.  
  c. Add the IP addresses of the media gateways that are controlled by the associated call agents to the group by entering them in Gateway to Be Added and clicking Add>>. Delete any gateways that are no longer used.  
  A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Normally, a gateway sends commands to the default MGCP port for call agents, UDP 2727.  
  d. Add the IP addresses of the call agents that control the MGCP media gateways by entering them in Call Agent to Be Added and clicking Add>>. Delete any agents that are no longer needed.  
  Normally, a call agent sends commands to the default MGCP port for gateways, UDP 2427.  
  e. Click OK in the MGCP Group dialog box. Repeat the process to add other groups as needed. |
| Step 6 | Click OK in the MGCP Inspect Map dialog box.  
  You can now use the inspection map in an MGCP inspection service policy. |

Configure the MGCP Inspection Service Policy

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.
**RTSP Inspection**

The following sections describe RTSP application inspection.

- RTSP Inspection Overview, page 9-12
- RealPlayer Configuration Requirements, page 9-13
- Limitations for RSTP Inspection, page 9-13
- Configure RTSP Inspection, page 9-14

**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.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the ASA keeps state and remembers the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

RTSP inspection does not support PAT or dual-NAT. Also, the 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 port` 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

RTSP inspection is enabled by default. You need to configure it only if you want non-default processing. If you want to customize RTSP inspection, use the following process.

Procedure

1. Configure RTSP Inspection Class Map, page 9-14
2. Configure RTSP Inspection Policy Map, page 9-15
3. Configure the RTSP Inspection Service Policy, page 9-16

Configure RTSP Inspection Class Map

You can optionally create an RTSP inspection class map to define the traffic class for RTSP inspection. The other option is to define the traffic classes directly in the RTSP inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.

Tip

You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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

1. Choose Configuration > Firewall > Objects > Class Maps > RTSP.
2. Do one of the following:
   - Click Add to add a new class map.
   - Select a map and click Edit.
3. For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
4. Choose a match option: Match All or Match Any.
   - Match All is the default, and specifies that traffic must match all criteria to match the class map. Match Any means that traffic matches the class map if it matches at least one criterion.
5. Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.
   - Choose the match type for the criteria: Match (traffic must match the criterion) or No Match (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.
   - Choose the match criterion and define its value:
     - URL Filter—Match the URL against the selected regular expression or regular expression class.
- Request Method—Match the request method: announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameters, teardown.

c. Click OK.

Step 6

Click OK in the RTSP Traffic Class Map dialog box.

You can now use the class map in a RTSP inspection policy map.

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.

Tip

You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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

Choose Configuration > Firewall > Objects > Inspect Maps > RTSP.

Step 2

Do one of the following:
- Click Add to add a new map.
- Select a map to and click Edit.

Step 3

For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4

Click the Parameters tab and configure the desired options:
- Enforce Reserve Port Protection—Whether to restrict the use of reserved ports during media port negotiation.
- Maximum URL Length—The maximum length of the URL allowed in the message, 0 to 6000.

Step 5

Click the Inspections tab and define the specific inspections you want to implement based on traffic characteristics.

You can define traffic matching criteria based on RTSP class maps, by configuring matches directly in the inspection map, or both.

a. Do any of the following:
- Click Add to add a new criterion.
- Select an existing criterion and click Edit.

b. Choose Single Match to define the criterion directly, or Multiple Match, in which case you select the RTSP class map that defines the criteria (see Configure RTSP Inspection Class Map, page 9-14.)
c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the class map. Then, configure the criterion as follows:

- **URL Filter**—Match the URL against the selected regular expression or regular expression class.
- **Request Method**—Match the request method: announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameters, teardown.

d. Choose the action to take for matching traffic. For URL matching, you can drop the connection or log it, and you can enable logging of dropped connections. For Request Method matches, you can apply a rate limit in packets per second.

e. Click **OK** to add the inspection. Repeat the process as needed.

**Step 6**
Click **OK** in the RTSP Inspect Map dialog box.
You can now use the inspection map in an RTSP inspection service policy.

---

**Configure the RTSP Inspection Service Policy**

The default ASA configuration includes RTSP inspection on the default port applied globally on all interfaces. 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.

**Procedure**

**Step 1**
Choose **Configuration > Firewall > Service Policy**, and open a rule.
- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have an RTSP inspection rule, or a rule to which you are adding RTSP inspection, select it and click **Edit**.

**Step 2**
On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3**
Select **RTSP**.

**Step 4**
If you want non-default inspection, click **Configure** and choose whether to use the default map or to use an RTSP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure RTSP Inspection Policy Map, page 9-15.
Click **OK** in the Select RTSP Inspect Map dialog box to assign the map to the policy.

**Step 5**
Click **OK** or **Finish** to save the service policy rule.
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, page 9-17
- Limitations for SIP Inspection, page 9-17
- SIP Instant Messaging, page 9-18
- Default SIP Inspection, page 9-19
- Configure SIP Inspection, page 9-19
- Configure SIP Timeout Values, page 9-24

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.

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.

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:
SIP Inspection

- 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.

- 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.

SIP Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. SIP supports the Chat feature on Windows XP using Windows Messenger RTC Client version 4.7.0105 only. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes that time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.

Note: Only the Chat feature is supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

SIP inspection translates the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL_ID/FROM/TO from the SIP payload. These indices identify the call, the source, and the destination. This database contains the media addresses and media ports found in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. The ASA opens RTP/RTCP connections between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message; however, subsequent messages may not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be translated.
As a call is set up, the SIP session is in the “transient” state until the media address and media port is received from the called endpoint in a Response message indicating the RTP port the called endpoint listens on. If there is a failure to receive the response messages within one minute, the signaling connection is torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection remains until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface does not traverse the ASA, unless the ASA configuration specifically allows it.

**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**

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. If you want to customize SIP inspection, use the following process.

**Procedure**

- **Step 1** Configure SIP Inspection Class Map, page 9-20
- **Step 2** Configure SIP Inspection Policy Map, page 9-21
- **Step 3** Configure the SIP Inspection Service Policy, page 9-23
Configure SIP Inspection Class Map

You can optionally create a SIP inspection class map to define the traffic class for SIP inspection. The other option is to define the traffic classes directly in the SIP inspection policy map. The difference between creating a class map and defining the traffic match directly in the inspection map is that you can create more complex match criteria and you can reuse class maps.

Tip

You can configure class maps while creating inspection maps or service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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 Choose Configuration > Firewall > Objects > Class Maps > SIP.

Step 2 Do one of the following:

- Click Add to add a new class map.
- Select a map and click Edit.

Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 Choose a match option: Match All or Match Any.

Match All is the default, and specifies that traffic must match all criteria to match the class map. Match Any means that traffic matches the class map if it matches at least one criterion.

Step 5 Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: Match (traffic must match the criterion) or No Match (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map.

b. Choose the match criterion and define its value:

- Called Party—Match the called party, as specified in the To header, against the selected regular expression or regular expression class.
- Calling Party—Match the calling party, as specified in the From header, against the selected regular expression or regular expression class.
- Content Length—Match a SIP content header of a length greater than specified, between 0 and 65536 bytes.
- Content Type—Match the Content Type header, either the SDP type or a type that matches the selected regular expression or regular expression class.
- IM Subscriber—Match the SIP IM subscriber against the selected regular expression or regular expression class.
- Message Path—Match the SIP Via header against the selected regular expression or regular expression class.
Request Method—Match the SIP request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.

Third-Party Registration—Match the requester of a third-party registration against the selected regular expression or regular expression class.

URI Length—Match 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.

c. Click OK.

Step 6
Click OK in the SIP Traffic Class Map dialog box.
You can now use the class map in a SIP inspection policy map.

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.

Tip
You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

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
Choose Configuration > Firewall > Objects > Inspect Maps > SIP.

Step 2
Do one of the following:
- Click Add to add a new map.
- Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

Step 3
For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4
In the Security Level view of the SIP Inspect Map dialog box, select the level that best matches your desired configuration. The default level is Low.

If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for SIP inspection.

Step 5
If you need to customize the settings further, click Details, and do the following:
- Click the Filtering tab and choose whether to enable SIP instant messaging (IM) extensions or to permit non-SIP traffic on the SIP port.
- Click the IP Address Privacy tab and choose whether to hide the server and endpoint IP addresses.
c. Click the **Hop Count** tab and choose whether to ensure that the number of hops to the destination is greater than 0. This 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.

d. Click the **RTP Conformance** tab and choose whether to check RTP packets that are flowing on the pinholes for protocol conformance. If you check for conformance, you can also choose whether to limit the payload to audio or video, based on the signaling exchange.

e. Click the **SIP Conformance** tab and choose whether to enable state transition checking and strict validation of header fields. For each option you choose, select the action to take for non-conforming traffic (drop packet, drop connection, reset, or log) and whether to enable or disable logging.

f. Click the **Field Masking** tab and choose whether to inspect non-SIP URIs in Alert-Info and Call-Info headers and to inspect the server’s and endpoint’s software version in the User-Agent and Server headers. For each option you choose, select the action to take (mask or log) and whether to enable or disable logging.

g. Click the **TVS Server** tab and identify the Trust Verification Services servers, which enable Cisco Unified IP Phones to authenticate application servers during HTTPS establishment. You can identify up to four servers; enter their IP addresses separated by commas. 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. If the configuration uses a non-default port, enter the port number (in the range 1026 to 32768). The default port is 2445.

**Step 6**  
Click the **Inspections** tab and define the specific inspections you want to implement based on traffic characteristics.

You can define traffic matching criteria based on SIP class maps, by configuring matches directly in the inspection map, or both.

a. Do any of the following:
   * Click **Add** to add a new criterion.
   * Select an existing criterion and click **Edit**.

b. Choose **Single Match** to define the criterion directly, or **Multiple Match**, in which case you select the SIP class map that defines the criteria (see **Configure SIP Inspection Class Map**, page 9-20.)

c. If you are defining the criterion here, choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). For example, if No Match is selected on the string “example.com,” then any traffic that contains “example.com” is excluded from the class map. Then, configure the criterion as follows:
   * Called Party—Match the called party, as specified in the To header, against the selected regular expression or regular expression class.
   * Calling Party—Match the calling party, as specified in the From header, against the selected regular expression or regular expression class.
   * Content Length—Match a SIP content header of a length greater than specified, between 0 and 65536 bytes.
   * Content Type—Match the Content Type header, either the SDP type or a type that matches the selected regular expression or regular expression class.
   * IM Subscriber—Match the SIP IM subscriber against the selected regular expression or regular expression class.
   * Message Path—Match the SIP Via header against the selected regular expression or regular expression class.
Chapter 9  Inspection for Voice and Video Protocols

SIP Inspection

- Request Method—Match the SIP request method: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- Third-Party Registration—Match the requester of a third-party registration against the selected regular expression or regular expression class.
- URI Length—Match 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. Choose the action to take for matching traffic (drop packet, drop connection, reset, log) and whether to enable or disable logging. For Request Method matches to “invite” and “register,” you can also apply a rate limit in packets per second.

e. Click OK to add the inspection. Repeat the process as needed.

Step 7

Click OK in the SIP Inspect Map dialog box.

You can now use the inspection map in a SIP inspection service policy.

Configure the SIP Inspection Service Policy

The default ASA configuration includes SIP inspection on the default port applied globally on all interfaces. 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.

Procedure

Step 1

Choose Configuration > Firewall > Service Policy, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.
- To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have a SIP inspection rule, or a rule to which you are adding SIP inspection, select it and click Edit.

Step 2

On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

Step 3

Select SIP.

Step 4

If you want non-default inspection, click Configure and do the following:

a. Choose whether to use the default map or to use a SIP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure SIP Inspection Policy Map, page 9-21.

b. If you want to inspect encrypted SIP traffic, choose Enable encrypted traffic inspection and select a TLS proxy (click Manage to create one if necessary).

Although you can select Phone Proxy or UC-IME Proxy to associate the TLS proxy with those proxies, this configuration is no longer recommended. Only one TLS proxy can be assigned to the Phone Proxy or UC-IME Proxy at a time. If you configure more than one service policy rule for Phone Proxy or UC-IME Proxy inspection and attempt to assign a different TLS proxy to them, ASDM displays a warning that all other service policy rules with Phone Proxy or UC-IME inspection will be changed to use the latest selected TLS proxy.
Skinny (SCCP) Inspection

The UC-IME Proxy configuration requires two TLS proxies – one for outbound traffic and one for inbound. Rather than associating the TLS proxies directly with the UC-IME Proxy, as is the case with phone proxy, the TLS proxies are associated with it indirectly via SIP inspection rules.

c. Click **OK** in the Select SIP Inspect Map dialog box.

---

**Step 5**

Click **OK** or **Finish** to save the service policy rule.

---

**Configure SIP Timeout Values**

The media connections are torn down within two minutes after the connection becomes idle. This is, however, a configurable timeout and can be set for a shorter or longer period of time.

You can configure several SIP global timeout values on the **Configuration > Firewall > Advanced > Global Timeouts** page.

**Skinny (SCCP) Inspection**

The following sections describe SCCP application inspection.

- SCCP Inspection Overview, page 9-24
- Supporting Cisco IP Phones, page 9-25
- Limitations for SCCP Inspection, page 9-25
- Default SCCP Inspection, page 9-25
- Configure SCCP (Skinny) Inspection, page 9-26

**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. An static identity entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an 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 currently 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 SCCP (Skinny) 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. If you want to customize SCCP inspection, use the following process.

Procedure

Step 1 Configure a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control, page 9-26.
Step 2 Configure the SCCP Inspection Service Policy, page 9-27.

Configure a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control

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 Choose Configuration > Firewall > Objects > Inspect Maps > SCCP (Skinny).
Step 2 Do one of the following:
   - Click Add to add a new map.
   - Select a map to view its contents. You can change the security level directly, or click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.
Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
Step 4 In the Security Level view of the SCCP (Skinny) Inspect Map dialog box, select the level that best matches your desired configuration. The default level is Low.
   - If one of the preset levels matches your requirements, you are now done. Just click OK, skip the rest of this procedure, and use the map in a service policy rule for SCCP inspection.
Step 5 If you need to customize the settings further, click Details, and do the following:
   - Click the Parameters tab and choose among the following options:
     - Enforce endpoint registration—Whether Skinny endpoints must register before placing or receiving calls.
     - Maximum Message ID—The maximum SCCP station message ID allowed. The default maximum is 0x181. The hex number can be 0x0 to 0xffff.
     - SCCP Prefix Length—The maximum and minimum SCCP prefix length. The default minimum is 4; there is no default maximum.
     - Timeouts—Whether to set timeouts for media and signaling connections, and the value of those timeouts. The defaults are 5 minutes for media, 1 hour for signaling.
b. Click the **RTP Conformance** tab and choose whether to check RTP packets that are flowing on the pinholes for protocol conformance. If you check for conformance, you can also choose whether to limit the payload to audio or video, based on the signaling exchange.

**Step 6** (Optional) Click the **Message ID Filtering** tab to identify traffic to drop based on the station message ID field in SCCP messages.

a. Do any of the following:
   - Click **Add** to add a new criterion.
   - Select an existing criterion and click **Edit**.

b. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion).

c. In the **Value** fields, identify the traffic based on the station message ID value in hexadecimal, from 0x0 to 0xffff. Either enter the value for a single message ID, or enter the beginning and ending value for a range of IDs.

d. Choose whether to enable or disable logging. The action is always to drop the packet.

e. Click **OK** to add the filter. Repeat the process as needed.

**Step 7** Click **OK** in the SCCP (Skinny) Inspect Map dialog box.

You can now use the inspection map in an SCCP inspection service policy.

---

### Configure the SCCP Inspection Service Policy

The default ASA configuration includes SCCP inspection on the default port applied globally on all interfaces. 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.

**Procedure**

**Step 1** Choose **Configuration > Firewall > Service Policy**, and open a rule.
   - To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.
   - To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic**, page 1-10.
   - If you have an SCCP inspection rule, or a rule to which you are adding SCCP inspection, select it and click **Edit**.

**Step 2** On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 3** Select SCCP (Skinny).

**Step 4** If you want non-default inspection, click **Configure** and do the following:

a. Choose whether to use the default map or to use an SCCP inspection policy map that you configured. You can create the map at this time. For detailed information, see **Configure a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control**, page 9-26.

b. If you want to inspect encrypted SCCP traffic, choose **Enable encrypted traffic inspection** and select a TLS proxy (click **Manage** to create one if necessary).
Although you can also use a Phone Proxy configured on the ASA to inspect Skinny application traffic, this configuration is no longer recommended.

**c.** Click **OK** in the Select SCCP Inspect Map dialog box.

**Step 5** Click **OK** or **Finish** to save the service policy rule.

---

### 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 ASDM screens.</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 Trust Verification Services Server support to the SIP inspection policy map.</td>
</tr>
</tbody>
</table>
The following topics explain application inspection for database and directory 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, page 7-1.

- ILS Inspection, page 10-1
- SQL*Net Inspection, page 10-2
- Sun RPC Inspection, page 10-3

ILS Inspection

The ILS inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The ASA supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the ASA border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

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/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST
and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:
- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions.
- Parses the LDAP packet.
- Extracts IP addresses.
- Translates IP addresses as necessary.
- Encodes the PDU with translated addresses using BER encode functions.
- Copies the newly encoded PDU back to the TCP packet.
- Performs incremental TCP checksum and sequence number adjustment.

ILS inspection has the following limitations:
- Referral requests and responses are not supported.
- Users in multiple directories are not unified.
- Single users having multiple identities in multiple directories cannot be recognized by NAT.

For information on enabling ILS inspection, see Configure Application Layer Protocol Inspection, page 7-8.

**SQL*Net Inspection**

SQL*Net inspection is enabled by default.

The SQL*Net protocol consists of different packet types that the ASA handles to make the data stream appear consistent to the Oracle applications on either side of the ASA.

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).

---

**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.

The ASA translates all addresses and looks in the packets for all embedded ports to open for SQL*Net Version 1.

For SQL*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

\[(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))\]

SQL*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the ASA, a flag will be set in the...
connection data structure to expect the Data or Redirect message that follows to be translated and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be translated and port connections will be opened.

For information on enabling SQL*Net inspection, see Configure Application Layer Protocol Inspection, page 7-8.

Sun RPC Inspection

This section describes Sun RPC application inspection.

- Sun RPC Inspection Overview, page 10-3
- Identifying Allowed Sun RPC Services, page 10-4

Sun RPC Inspection Overview

The Sun RPC inspection engine enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access 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.

Tip

Sun RPC 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. For information on enabling Sun RPC inspection, see Configure Application Layer Protocol Inspection, page 7-8.

The following limitations apply to Sun RPC inspection:

- NAT or PAT of Sun RPC payload information is not supported.
- Sun RPC inspection supports inbound ACLs only. Sun RPC inspection does not support outbound ACLs because the inspection engine uses dynamic ACLs instead of secondary connections. Dynamic ACLs are always added on the ingress direction and not on egress; therefore, this inspection engine does not support outbound ACLs. To view the dynamic ACLs configured for the ASA, use the show asp table classify domain permit command.
Identifying Allowed Sun RPC Services

You need to identify the Sun RPC servers and services that you want to allow through the firewall. Sun RPC inspection uses this table when evaluating traffic.

**Procedure**

**Step 1** Choose **Configuration > Firewall > Advanced > SUNRPC Server**.

**Step 2** Do one of the following:
- Click **Add** to add a new server.
- Select a server and click **Edit**.

**Step 3** Configure the service properties:
- **Interface Name**—The interface through which traffic to the server flows.
- **IP Address/Mask**—The address of the Sun RPC server.
- **Service ID**—The service type on the server. 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**—Whether the service uses TCP or UDP.
- **Port/Port Range**—The port or range of ports used by the service.
- **Timeout**—The idle timeout for the connection.

**Step 4** Click **OK**.
Inspection for Management Application Protocols

The following topics explain application inspection for management application 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, page 7-1.

Several common inspection engines are enabled on the ASA by default, but you might need to enable others depending on your network.

- DCERPC Inspection, page 11-1
- GTP Inspection, page 11-4
- RADIUS Accounting Inspection, page 11-8
- RSH Inspection, page 11-11
- SNMP Inspection, page 11-11
- XDMCP Inspection, page 11-12

DCERPC Inspection

The following sections describe the DCERPC inspection engine.

- DCERPC Overview, page 11-1
- Configure DCERPC Inspection, page 11-2

DCERPC Overview

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The security appliance allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.
DCERPC inspection maps inspect for native TCP communication between the EPM and client on well-known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have configurable timeouts.

**Note**

DCERPC inspection only supports communication between the EPM and clients to open pinholes through the ASA. Clients using RPC communication that does not use the EPM is not supported with DCERPC inspection.

### Configure DCERPC Inspection

DCERPC inspection is not enabled by default. You must configure it if you want DCERPC inspection.

**Procedure**

**Step 1** Configure a DCERPC Inspection Policy Map, page 11-2.

**Step 2** Configure the DCERPC Inspection Service Policy, page 11-3.

### 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.

**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** Choose Configuration > Firewall > Objects > Inspect Maps > DCERPC.

**Step 2** Do one of the following:

- Click **Add** to add a new map.
- Select a map to view its contents. You can change the security level directly, or click **Customize** to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

**Step 3** For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

**Step 4** In the **Security Level** view of the DCERPC Inspect Map dialog box, select the level that best matches your desired configuration.

If one of the preset levels matches your requirements, you are now done. Just click **OK**, skip the rest of this procedure, and use the map in a service policy rule for DCERPC inspection.

If you need to customize the settings further, click **Details**, and continue with the procedure.
Step 5 Configure the desired options.

- **Pinhole Timeout**—Sets the pinhole timeout. Because a client may use the server information returned by the endpoint mapper for multiple connections, the timeout value is configurable based on the client application environment. Range is from 0:0:1 to 1193:0:0.

- **Enforce endpoint-mapper service**—Whether to enforce the endpoint mapper service during binding so that only its service traffic is processed.

- **Enable endpoint-mapper service lookup**—Whether to enable the lookup operation of the endpoint mapper service. You can also enforce a timeout for the service lookup. If you do not configure a timeout, the pinhole timeout is used.

Step 6 Click **OK**.

You can now use the inspection map in a DCERPC inspection service policy.

---

**Configure the DCERPC Inspection Service Policy**

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.

**Procedure**

Step 1 Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.

- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic**, page 1-10.

- If you have an DCERPC inspection rule, or a rule to which you are adding DCERPC inspection, select it and click **Edit**.

Step 2 On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

Step 3 (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the DCERPC inspection, and then re-enable it with the new inspection policy map name:

a. Uncheck the **DCERPC** check box.

b. Click **OK**.

c. Click **Apply**.

d. Repeat these steps to return to the Protocol Inspections tab.

Step 4 Select **DCERPC**.

Step 5 If you want non-default inspection, click **Configure**, and do the following:

a. Choose whether to use the default map or to use a DCERPC inspection policy map that you configured. You can create the map at this time. For detailed information, see **Configure a DCERPC Inspection Policy Map**, page 11-2.

b. Click **OK** in the Select DCERPC Inspect Map dialog box.
Step 6

Click **OK** or **Finish** to save the service policy rule.

---

**GTP Inspection**

The following sections describe the GTP inspection engine.

---

**Note**

GTP inspection requires a special license.

---

- GTP Inspection Overview, page 11-4
- Defaults for GTP Inspection, page 11-5
- Configure GTP Inspection, page 11-5

---

**GTP Inspection Overview**

GPRS provides uninterrupted connectivity for mobile subscribers between GSM networks and corporate networks or the Internet. The GGSN is the interface between the GPRS wireless data network and other networks. The SGSN performs mobility, data session management, and data compression.

![GPRS Tunneling Protocol](image)

The UMTS is the commercial convergence of fixed-line telephony, mobile, Internet and computer technology. UTRAN is the networking protocol used for implementing wireless networks in this system. GTP allows multi-protocol packets to be tunneled through a UMTS/GPRS backbone between a GGSN, an SGSN and the UTRAN.

GTP does not include any inherent security or encryption of user data, but using GTP with the ASA helps protect your network against these risks.
The SGSN is logically connected to a GGSN using GTP. GTP allows multiprotocol packets to be tunneled through the GPRS backbone between GSNs. GTP provides a tunnel control and management protocol that allows the SGSN to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP uses a tunneling mechanism to provide a service for carrying user data packets.

**Note**

When using GTP with failover, if a GTP connection is established and the active unit fails before data is transmitted over the tunnel, the GTP data connection (with a “j” flag set) is not replicated to the standby unit. This occurs because the active unit does not replicate embryonic connections to the standby unit.

**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 which 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.
- The GSN timeout is 30 minutes.
- The PDP context timeout is 30 minutes.
- 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.

**Configure GTP Inspection**

GTP inspection is not enabled by default. You must configure it if you want GTP inspection.

**Procedure**

- **Step 1** Configure a GTP Inspection Policy Map, page 11-6.
- **Step 2** Configure the GTP Inspection Service Policy, page 11-8.
- **Step 3** (Optional) Configure RADIUS accounting inspection to protect against over-billing attacks. See RADIUS Accounting Inspection, page 11-8.
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**

1. Choose Configuration > Firewall > Objects > Inspect Maps > GTP.
2. Do one of the following:
   - Click Add to add a new map.
   - Select a map to view its contents. Click Customize to edit the map. The remainder of the procedure assumes you are customizing or adding a map.
3. For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.
4. In the Security Level view of the GTP Inspect Map dialog box, view the current configuration of the map.
   - The view indicates whether the map uses default values or if you have customized it. If you need to customize the settings further, click Details, and continue with the procedure.
5. Click the Permit Parameters tab and configure the desired options:
   - **Permit Response**—When the ASA performs GTP inspection, by default the ASA drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS.
     - To configure GSN pooling and thus support load balancing, create a network object group that specifies the GSNs and select this as a “From Object Group.” Likewise, create a network object group for the SGSN and select it as the “To Object Group.” If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in an object group that the responding GSN is permitted to send a GTP response to, the ASA permits the response.
     - The network object group can identify the GSN or SGSN by host address or by the subnet that contains them.
   - **Permit Errors**—Whether to allow packets that are invalid or that encountered an error during inspection to be sent through the ASA instead of being dropped.
6. Click the General Parameters tab and configure the desired options:
   - **Maximum Number of Requests**—The maximum number of GTP requests that will be queued waiting for a response.
   - **Maximum Number of Tunnels**—The maximum number of tunnels allowed.
• **Enforce Timeout**—Whether to enforce idle timeouts for the following behaviors. Timeouts are in hh:mm:ss format.
  - GSN—The maximum period of inactivity before a GSN is removed.
  - PDP-Context—The maximum period of inactivity before receiving the PDP Context for a GTP session.
  - Request—The maximum period of inactivity before receiving the GTP message during a GTP session.
  - Signaling—The maximum period of inactivity before GTP signaling is removed.
  - T3-Response timeout—The maximum wait time for a response before removing the connection.
  - Tunnel—The maximum period of inactivity for the GTP tunnel.

**Step 7** Click the **IMSI Prefix Filtering** tab and configure IMSI prefix filtering if desired.

By default, the security appliance 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 8** Click the **Inspections** tab and define the specific inspections you want to implement based on traffic characteristics.

a. Do any of the following:
   - Click **Add** to add a new criterion.
   - Select an existing criterion and click **Edit**.

b. Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). Then, configure the criterion:
   - **Access Point Name**—Matches the access point name against the specified regular expression or regular expression class. By default, all messages with valid access point names are inspected and any name is allowed.
   - **Message ID**—Matches the message ID, from 1 to 255. You can specify one value or a range of values. By default, all valid message IDs are allowed.
   - **Message Length**—Matches messages where the length of the UDP payload is between the specified minimum and maximum length.
   - **Version**—Matches the GTP version, from 0 to 255. You can specify one value or a range of values. Version 0 of GTP uses port 3386, while Version 1 uses port 2123. By default all GTP versions are allowed.

c. For Message ID matching, choose whether to drop the packet or to apply a rate limit in packets per second. The action for all other matches is to drop the packet. For all matches, you can choose whether to enable logging.

d. Click **OK** to add the inspection. Repeat the process as needed.

**Step 9** Click **OK** in the GTP Inspect Map dialog box.
RADIUS Accounting Inspection

You can now use the inspection map in a GTP inspection service policy.

Configure the GTP Inspection Service Policy

GTP 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 GTP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

Procedure

Step 1
Choose Configuration > Firewall > Service Policy, and open a rule.
- To edit the default global policy, select the “inspection_default” rule in the Global folder and click Edit.
- To create a new rule, click Add > Add Service Policy Rule. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have a GTP inspection rule, or a rule to which you are adding GTP inspection, select it and click Edit.

Step 2
On the Rule Actions wizard page or tab, select the Protocol Inspection tab.

Step 3
(To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the GTP inspection, and then re-enable it with the new inspection policy map name:
- Uncheck the GTP check box.
- Click OK.
- Click Apply.
- Repeat these steps to return to the Protocol Inspections tab.

Step 4
Select GTP.

Step 5
If you want non-default inspection, click Configure, and do the following:
- Choose whether to use the default map or to use a GTP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure a GTP Inspection Policy Map, page 11-6.
- Click OK in the Select GTP Inspect Map dialog box.

Step 6
Click OK or Finish to save the service policy rule.

RADIUS Accounting Inspection

The following sections describe the RADIUS Accounting inspection engine.
- RADIUS Accounting Inspection Overview, page 11-9
- Configure RADIUS Accounting Inspection, page 11-9
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 GTP/GPRS 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.

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, page 11-9.
Step 2 Configure the RADIUS Accounting Inspection Service Policy, page 11-10.

Configure a RADIUS Accounting Inspection Policy Map

You must create a RADIUS accounting inspection policy map to configure the attributes needed for the inspection.

Tip

You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.
### Procedure

**Step 1** Choose **Configuration > Firewall > Objects > Inspect Maps > RADIUS Accounting**.

**Step 2** Do one of the following:
- Click **Add** to add a new map.
- Select a map and click **Edit**.

**Step 3** For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

**Step 4** Click the **Host Parameters** tab and add the IP addresses of each 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. The ASA receives a copy of the RADIUS accounting messages from these hosts.

**Step 5** Click the **Other Parameters** tab and configure the desired options.
- **Send responses to the originator of the RADIUS accounting message**—Whether to mask the banner from the ESMTP server.
- **Enforce user timeout**—Whether to implement an idle timeout for users, and the timeout value. The default is one hour.
- **Enable detection of GPRS accounting**—Whether to 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**—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](http://www.iana.org/assignments/radius-types).

**Step 6** Click **OK**.

You can now use the inspection map in a RADIUS accounting inspection service policy.

### 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** Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To create a new rule, click **Add > Add Management Service Policy Rule**. Proceed through the wizard to the Rule Actions page according to **Add a Service Policy Rule for Management Traffic, page 1-13**.

- If you have a RADIUS accounting inspection rule, or a management rule to which you are adding RADIUS accounting inspection, select it, click **Edit**, and click the **Rule Actions** tab.

**Step 2** (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the RADIUS accounting inspection, and then re-enable it with the new inspection policy map name:

1. Select **None** for the RADIUS Accounting map.
2. Click **OK**.
3. Click **Apply**.
4. Repeat these steps to return to the Protocol Inspections tab.

**Step 3** Choose the desired **RADIUS Accounting Map**. You can create the map at this time. For detailed information, see **Configure a RADIUS Accounting Inspection Policy Map, page 11-9**.

**Step 4** Click **OK** or **Finish** to save the management service policy rule.

---

**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, page 7-8**.

**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**

**Step 1** Choose **Configuration > Firewall > Objects > Inspect Maps > SNMP** and do the following:

a. Click **Add**, or select a map and click **Edit**. When adding a map, enter a map name.

b. Select the SNMP versions to disallow.

c. Click **OK**.

**Step 2** Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To edit the default global policy, select the “inspection_default” rule in the Global folder and click **Edit**.

- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to **Add a Service Policy Rule for Through Traffic, page 1-10**.

- If you have an SNMP inspection rule, or a rule to which you are adding SNMP inspection, select it and click **Edit**.

**Step 3** On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

**Step 4** (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the SNMP inspection, and then re-enable it with the new inspection policy map name:

a. Uncheck the **SNMP** check box.

b. Click **OK**.

c. Click **Apply**.

d. Repeat these steps to return to the Protocol Inspections tab.

**Step 5** Select **SNMP**.

**Step 6** If you want non-default inspection, click **Configure**, and do the following:

a. Choose whether to use the default map (which allows all versions) or to use a SNMP inspection policy map that you configured. You can create the map at this time.

b. Click **OK** in the Select SNMP Inspect Map dialog box.

**Step 7** Click **OK** or **Finish** to save the service policy rule.

---

**XDMCP Inspection**

XDMCP inspection is enabled by default; however, the XDMCP inspection engine is dependent upon proper configuration of the **established** command.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the ASA must allow the TCP back connection from the Xhosted computer. To permit the back connection, 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, page 7-8.
PART 4

Connection Settings and Quality of Service
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?, page 12-1
- Configure Connection Settings, page 12-2
- Monitoring Connections, page 12-13
- History for Connection Settings, page 12-14

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 includes counters to show the amount of activity from DCD.
**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.

TCP Intercept, TCP State Bypass, and Dead Connection Detection (DCD) are not enabled. You would configure these services on specific traffic classes only, and not as a general service.

The following general procedure covers the gamut of possible connection setting configurations. Pick and choose which to implement based on your needs.

**Procedure**

**Step 1** Configure Global Timeouts, page 12-3. 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.

**Step 2** Protect Servers from a SYN Flood DoS Attack (TCP Intercept), page 12-4. Use this procedure to configure TCP Intercept.

**Step 3** Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer), page 12-6, if you want to alter the default TCP Normalization behavior for specific traffic classes.

**Step 4** Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass), page 12-8, if you have this type of routing environment.

**Step 5** Disable TCP Sequence Randomization, page 12-10, if the default randomization is scrambling data for certain connections.

**Step 6** Configure Connection Settings for Specific Traffic Classes (All Services), page 12-11. 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 TCP Intercept, Dead Connection Detection, or TCP State Bypass.
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. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

Changing the global timeout sets a new default timeout, which in some cases can be overridden for particular traffic flows through service policies.

**Procedure**

**Step 1** Choose Configuration > Firewall > Advanced > Global Timeouts.

**Step 2** Configure the timeouts by checking the boxes for timeouts you want to change and entering the new value.

All durations are displayed in the format `hh:mm:ss`, with a maximum duration of 1193:0:0. In all cases, except for Authentication absolute and Authentication inactivity, unchecking the check boxes returns the timeout to the default value. For those two cases, clearing the check box means to reauthenticate on every new connection.

Enter 0 to disable a timeout.

- **Connection**—The idle time until a connection slot is freed. This duration must be at least 5 minutes. The default is 1 hour.
- **Half-closed**—The idle time until a TCP half-closed connection closes. The minimum is 5 minutes. The default is 10 minutes.
- **UDP**—The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.
- **ICMP**—The idle time after which general ICMP states are closed. The default (and minimum) is 2 seconds.
- **H.323**—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.
- **H.225**—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.
- **MGCP**—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).
- **MGCP PAT**—The idle time after which an MGCP PAT translation is removed. The default is 5 minutes (0:5:0). The minimum time is 30 seconds.
- **TCP Proxy Reassembly**—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).
- **Floating Connection**—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 between 0:1:0 and 1193:0:0.
- **SUNRPC**—The idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.
Configure Connection Settings

- **SIP**—The idle time until an SIP signaling port connection closes. This duration must be at least 5 minutes. The default is 30 minutes.
- **SIP Media**—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.
- **SIP Provisional Media**—The timeout value for SIP provisional media connections, between 0:1:0 and 1193:0:0. The default is 2 minutes.
- **SIP Invite**—The idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 00:30:0. The default is 3 minutes (0:3:0).
- **SIP Disconnect**—The idle time after which SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message. The minimum value is 0:0:1, the maximum value is 0:10:0. The default value is 0:2:0.
- **Authentication absolute**—The duration until the authentication cache times out and users have to reauthenticate a new connection. This duration must be shorter than the Translation Slot value. The system waits until the user starts a new connection to prompt again. Before entering 0:0:0 to disable caching and reauthenticate on every new connection, consider the following limitations:
  - Do not set this value to 0:0:0 if passive FTP is used on the connections.
  - When Authentication Absolute is 0, HTTPS authentication may not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is permitted through, but subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even after successful authentication. To work around this, set the authentication absolute timeout to 1 second. This workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.
- **Authentication inactivity**—The idle time until the authentication cache times out and users have to reauthenticate a new connection. This duration must be shorter than the Translation Slot value.
- **Translation Slot**—The idle time until a translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.
- **(8.4(3) and later, not including 8.5(1) and 8.6(1)) PAT Translation Slot**—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.

**Step 3**  
Click **Apply**.

---

**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.

Note

Ensure that you set the embryonic connection limit lower than the TCP SYN backlog queue on the server that you want to protect. Otherwise, valid clients can no longer access the server during a SYN attack. To determine reasonable values for embryonic limits, carefully analyze the capacity of the server, the network, and server usage.

The 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 Choose Configuration > Firewall > Service Policy.

Step 2 Click Add > Add Service Policy Rule.

Alternatively, if you already have a rule for the servers you want to protect, edit the rule.

Step 3 Select whether to apply the rule to a specific interface or globally to all interfaces, and click Next.

Step 4 For Traffic Classification, select Source and Destination IP Addresses (uses ACL) and click Next.

Step 5 For the ACL rule, enter the IP addresses of the servers in Destination, and specify the protocol for the servers. Typically, you would use any for the Source. Click Next when finished.

For example, if you want to protect the web servers 10.1.1.5 and 10.1.1.6, enter:

- Source = any
- Destination = 10.1.1.5, 10.1.1.6
- Destination Protocol = tcp/http

Step 6 On the Rule Actions page, click the Connection Settings tab and fill in these options:

- Embryonic Connections—The maximum number of embryonic connections per host up to 2000000. The default is 0, which means the maximum embryonic connections are allowed. For example, you could set this to 1000.
Configure Connection Settings

- **Per Client Embryonic Connections**—The maximum number of simultaneous TCP embryonic connections for each client up to 2000000. When a new TCP connection is requested by a client that already has the maximum per-client number of embryonic connections open through the ASA, the ASA prevents the connection. For example, you could set this to 50.

**Step 7**  Click **Finish** to save the rule, and **Apply** to update the device.

**Step 8**  Choose **Configuration > Firewall > Threat Detection**, and enable at least the **TCP Intercept** statistics under the Threat Detection Statistics group.

You can simply enable all statistics, or just enable TCP Intercept. You can also adjust the monitoring window and rates.

**Step 9**  Choose **Home > Firewall Dashboard**, and look at the **Top Ten Protected Servers under SYN Attack** dashboard to monitor the results.

Click the **Detail** button to show 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.

You can clear the statistics by entering the **clear threat-detection statistics tcp-intercept** command using **Tools > Command Line Interface**.

---

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.

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**  Choose **Configuration > Firewall > Objects > TCP Maps**.

**Step 2**  Do one of the following:

- Click **Add** to add a new TCP map. Enter a name for the map.
- Select a map and click **Edit**.

**Step 3**  In the **Queue Limit** field, enter the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, between 0 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, IPS, and TCP check-retransmission 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 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.
Step 4  In the **Timeout** field, set the maximum amount of time that out-of-order packets can remain in the buffer, between 1 and 20 seconds.

If they are not put in order and passed on within the timeout period, then they are dropped. The default is 4 seconds. You cannot change the timeout for any traffic if the **Queue Limit** is set to 0; you need to set the limit to be 1 or above for the Timeout to take effect.

Step 5  For **Reserved Bits**, select how to handle packets that have reserved bits in the TCP header: **Clear and allow** (remove the bits before allowing the packet), **Allow only** (do not change the bits, the default), or **Drop** the packet.

Step 6  Select any of the following options:

- **Clear urgent flag**—Clears the URG flag in a packet before allowing it. The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks.

- **Drop connection on window variation**—Drops a connection that has changed its window size unexpectedly. The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged.

- **Drop packets that exceed maximum segment size**—Drops packets that exceed the MSS set by the peer.

- **Check if transmitted data is the same as original**—Enables the retransmit data checks, which prevent inconsistent TCP retransmissions.

- **Drop packets which have past-window sequence**—Drops packets that have past-window sequence numbers, namely the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window. To allow these packets, deselect this option and set the **Queue Limit** to 0 (disabling the queue limit).

- **Drop SYN Packets with data**—Drops SYN packets that contain data.

- **Enable TTL Evasion Protection**—Protects against TTL evasion attacks. 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.

- **Verify TCP Checksum**—Verifies the TCP checksum, dropping packets that fail verification.

- **Drop SYNAACK Packets with data**—Drops TCP SYNAACK packets that contain data.

- **Drop packets with invalid ACK**—Drops packets with an invalid ACK. You might see invalid ACKs in the following instances:
  - In the TCP connection SYN-ACK-received status, if the ACK number of a received TCP packet is not exactly same as the sequence number of the next TCP packet sending out, it is an invalid ACK.
  - Whenever the ACK number of a received TCP packet is greater than the sequence number of the next TCP packet sending out, it is an invalid ACK.

**Note**  TCP packets with an invalid ACK are automatically allowed for WAAS connections.
Configure Connection Settings

**Step 7** Set the action for packets that contain TCP options. You can clear the options before allowing the packets, or allow the packets without change. The default is to allow the three named options, while clearing all other options.

- **Clear Selective Ack**—Clears the selective acknowledgment mechanism option.
- **Clear TCP Timestamp**—Clears the TCP timestamp. Clearing the timestamp option disables PAWS and RTT.
- **Clear Window Scale**—Clears the window scale mechanism option.
- **Range**—Sets the action for unnamed options. The ranges can be within 6-7 and 9-255. Choose **Allow** or **Delete** (that is, clear) for each range.

**Step 8** Click **OK** and **Apply**.

You can now use the TCP map in a service policy. The map affects traffic only when applied through a service policy.

**Step 9** Apply the TCP map to a traffic class using a service policy.

a. Choose **Configuration > Firewall > Service Policy Rules**.

b. Add or edit a rule. You can apply the rule globally or to an interface. For example, to customize abnormal packet handling for all traffic, create a global rule that matches any traffic. Proceed to the **Rule Actions** page.

c. Click the **Connection Settings** tab.

d. Choose **Use TCP Map** and select the map you created.

e. Click **Finish** or **OK**, then click **Apply**.

### 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**, page 12-8
- **Guidelines for TCP State Bypass**, page 12-9
- **Configure TCP State Bypass**, page 12-10

### 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 (is this a new connection or an 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). See the general operations configuration guide for more detailed information about the stateful firewall.
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 ASA 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 ASA 1, then the packets will match the entry in the fast path, and are passed through. But if subsequent packets go to ASA 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:

![Asymmetric Routing](image)

If you have asymmetric routing configured on upstream routers, and traffic alternates between two ASAs, 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 an 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 for TCP State Bypass

**TCP State Bypass Unsupported Features**

The following features are not supported when you use TCP state bypass:

- Application inspection—Application inspection requires both inbound and outbound traffic to go through the same ASA, so application inspection is applied 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.
Configure Connection Settings

- 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 an any type of service module, such as IPS or CX.
- 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 ASAs for TCP state bypass traffic. If you use dynamic NAT, the address chosen for the session on ASA 1 will differ from the address chosen for the session on ASA 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.

Procedure

Step 1 Choose Configuration > Firewall > Service Policy.
Step 2 Click Add > Add Service Policy Rule.
Alternatively, if you already have a rule for the hosts, edit the rule.
Step 3 Select whether to apply the rule to a specific interface or globally to all interfaces, and click Next.
Step 4 For Traffic Classification, select Source and Destination IP Addresses (uses ACL) and click Next.
Step 5 For the ACL rule, enter the IP addresses of the hosts on each end of the route in Source and Destination, and specify the protocol as TCP. Click Next when finished.
For example, if you want to bypass TCP state checking between 10.1.1.1 and 10.2.2.2, enter:
- Source = 10.1.1.1
- Destination = 10.2.2.2
- Destination Protocol = tcp
Step 6 On the Rule Actions page, click the Connection Settings tab and select TCP State Bypass.
Step 7 Click Finish to save the rule, and Apply to update the device.

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.

Procedure

**Step 1** Choose **Configuration > Firewall > Service Policy**.

**Step 2** Click **Add > Add Service Policy Rule**.
Alternatively, if you already have a rule for the targeted traffic, edit the rule.

**Step 3** Select whether to apply the rule to a specific interface or globally to all interfaces, and click **Next**.

**Step 4** For Traffic Classification, identify the type of traffic match. 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. Click **Next** and configure the hosts in the ACL or define the ports, and click **Next** again.

For example, if you want to disable TCP sequence number randomization for all TCP traffic directed at 10.2.2.2, enter:

- Source = any
- Destination = 10.2.2.2
- Destination Protocol = tcp

**Step 5** On the Rule Actions page, click the **Connection Settings** tab and uncheck **Randomize Sequence Number**.

**Step 6** Click **Finish** to save the rule, and **Apply** to update the device.

**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.
- Decrement time-to-live (TTL) on packets so that the ASA will show up on trace route output.

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.
Configure Connection Settings

**Tip**

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.

**Procedure**

**Step 1**

Choose **Configuration > Firewall > Service Policy**, and open a rule.

- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page according to Add a Service Policy Rule for Through Traffic, page 1-10.
- If you have a rule for which you are changing connection settings, select it and click **Edit**.

**Step 2**

On the Rule Actions wizard page or tab, select the **Connection Settings** tab.

**Step 3**

To set maximum connections, configure the following values in the Maximum Connections area:

- **TCP & UDP Connections**—The maximum number of simultaneous TCP and UDP connections for all clients in the traffic class, up to 2000000. The default is 0, which means the maximum possible connections are allowed.

- **Embryonic Connections**—Specifies the maximum number of embryonic connections per host up to 2000000. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. The default is 0, which means the maximum embryonic connections are allowed. 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.

- **Per Client Connections**—Specifies the maximum number of simultaneous TCP and UDP connections for each client up to 2000000. When a new connection is attempted by a client that already has opened the maximum per-client number of connections, the ASA rejects the connection and drops the packet.

- **Per Client Embryonic Connections**—Specifies the maximum number of simultaneous TCP embryonic connections for each client up to 2000000. When a new TCP connection is requested by a client that already has the maximum per-client number of embryonic connections open through the ASA, the ASA prevents the connection.

**Step 4**

To configure connection timeouts, configure the following values in the TCP Timeout area:

- **Embryonic Connection Timeout**—The idle time until an embryonic (half-open) connection slot is freed. Enter 0:0:0 to disable timeout for the connection. The default is 30 seconds.

- **Half Closed Connection Timeout**—The idle timeout period until a half-closed connection is closed, between 0:5:0 (for 9.1(1) and earlier) or 0:0:30 (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.

- **Connection Timeout**—The idle time until a connection slot (of any protocol, not just TCP) is freed. Enter 0:0:0 to disable timeout for the connection. This duration must be at least 5 minutes. The default is 1 hour.

- **Send reset to TCP endpoints before timeout**—Whether the ASA should send a TCP reset message to the endpoints of the connection before freeing the connection slot.
• **Dead Connection Detection (DCD)**—Whether to 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. Set the maximum number of retries (default is 5, the range is 1-255) and the retry interval, which is the period to wait after each unresponsive DCD probe before sending another probe (0:0:1 to 24:0:0, default is 0:0:15).

**Step 5**
To disable randomized sequence numbers, uncheck **Randomize Sequence Number**.
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.

**Step 6**
To customize TCP Normalizer behavior, check **Use TCP Map** and choose an existing TCP map from the drop-down list (if available), or add a new one by clicking **New**.

**Step 7**
To decrement time-to-live (TTL) on packets that match the class, check **Decrement time to live for a connection**.
Decrementing TTL is necessary for the ASA to show up in trace routes as one of the hops. You must also increase the rate limit for ICMP Unreachable messages on **Configuration > Device Management > Management Access > ICMP**.

**Step 8**
To enable TCP state bypass, check **TCP State Bypass**.

**Step 9**
Click **OK** or **Finish**.

---

**Monitoring Connections**

Use the following pages to monitor connections:

• **Home > Firewall Dashboard**, and look at the **Top Ten Protected Servers under SYN Attack** dashboard to monitor TCP Intercept. Click the **Detail** button to show 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.

• Monitoring > Properties > Connections, to see current connections.

• Monitoring > Properties > Connection Graphs, to monitor performance.

In addition, you can enter the following commands using **Tools > Command Line Interface**.

• **show conn**
Shows connection information. The “b” flag indicates traffic subject to TCP State Bypass.

• **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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following screen was modified: Configuration &gt; Firewall &gt; Service Policies &gt; Rule Actions &gt; Connection Settings.</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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 0 (the connection never times out). To take advantage of this feature, change the timeout to a new value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the new connection because the previous connection might still be open on the upstream device. The PAT xlate timeout is now configurable, to a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>value between 30 seconds and 5 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screen: Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>This feature is not available in 8.5(1) or 8.6(1).</em></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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Connection Settings.</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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>better DoS protection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration &gt; Firewall &gt; Service Policy Rules &gt; Connection Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</td>
</tr>
</tbody>
</table>
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.

Note
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.

This chapter describes how to apply QoS policies.
- About QoS, page 13-1
- Guidelines for QoS, page 13-3
- Configure QoS, page 13-4
- Monitor QoS, page 13-8
- History for QoS, page 13-10

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, page 13-2
- What is a Token Bucket?, page 13-2
- Policing, page 13-2
- Priority Queuing, page 13-3
- DSCP (DiffServ) Preservation, page 13-3
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, page 13-2 for more information.

- **Priority queuing**—For critical traffic that cannot tolerate latency, such as Voice over IP (VoIP), you can identify traffic for Low Latency Queuing (LLQ) so that it is always transmitted ahead of other traffic. See Priority Queuing, page 13-3.

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, page 13-6), 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.

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. See Feature Directionality, page 1-4 for more information.
- 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Determine the Queue and TX Ring Limits for a Priority Queue, page 13-4.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the Priority Queue for an Interface, page 13-6.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure a Service Rule for Priority Queuing and Policing, page 13-7.</td>
</tr>
</tbody>
</table>

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, page 13-4
- TX Ring Limit Worksheet, page 13-5

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, page 13-6.

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.
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 13-1 Queue Limit Worksheet

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Formula</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outbound bandwidth (Mbps or Kbps)</td>
<td>Mbps × 125</td>
<td># of bytes/ms</td>
</tr>
<tr>
<td>2</td>
<td>Average packet size (bytes)</td>
<td># of bytes/ms from Step 1 ÷ Maximum packet size (bytes) x Delay (ms)</td>
<td>Queue limit (# of packets)</td>
</tr>
</tbody>
</table>

### Table 13-2 TX Ring Limit Worksheet

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Formula</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outbound bandwidth (Mbps or Kbps)</td>
<td>Mbps × 125</td>
<td># of bytes/ms</td>
</tr>
<tr>
<td>2</td>
<td>Maximum packet size (bytes)</td>
<td># of bytes/ms from Step 1 ÷ Maximum packet size (bytes) x Delay (ms)</td>
<td>TX ring limit (# of packets)</td>
</tr>
</tbody>
</table>
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
Choose Configuration > Device Management > Advanced > Priority Queue, and click Add.

Step 2
Configure the following options:

- **Interface**—The physical interface name on which you want to enable the priority queue, or for the ASASM, the VLAN interface name.
- **Queue Limit**—The number of average, 256-byte packets that the specified interface can transmit in a 500-ms interval.
  
  A packet that stays more than 500 ms in a network node might trigger a timeout in the end-to-end application. Such a packet can be discarded in each network node.
  
  Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped (called *tail drop*). To avoid having the queue fill up, you can use this option to increase the queue buffer size.
  
  The upper limit of the range of values for this option is determined dynamically at run time. The key determinants are the memory needed to support the queues and the memory available on the device.
  
  The Queue Limit that you specify affects both the higher priority low-latency queue and the best effort queue.
- **Transmission Ring Limit**—The depth of the priority queues, which is the number of maximum 1550-byte packets that the specified interface can transmit in a 10-ms interval.
  
  This setting guarantees that the hardware-based transmit ring imposes no more than 10-ms of extra latency for a high-priority packet.
  
  This option sets the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears.
  
  The upper limit of the range of values is determined dynamically at run time. The key determinants are the memory needed to support the queues and the memory available on the device.
  
  The Transmission Ring Limit that you specify affects both the higher priority low-latency queue and the best-effort queue.

Step 3
Click OK.

Step 4
Click Apply.
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, page 13-3 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
Choose Configuration > Firewall > Service Policy, and open a rule.
You can configure QoS as part of a new service policy rule, or you can edit an existing service policy.

Step 2
Proceed through the wizard to the Rules page, selecting the interface (or global) and traffic matching criteria along the way.
For policing traffic, you can choose to police all traffic that you are not prioritizing, or you can limit the traffic to certain types.

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.

For detailed information service policy rules, see Chapter 1, “Service Policy.”

Step 3
In the Rule Actions dialog box, click the QoS tab.

Step 4
Select Enable priority for this flow.
If this service policy rule is for an individual interface, ASDM automatically creates the priority queue for the interface (Configuration > Device Management > Advanced > Priority Queue; for more information, see Configure the Priority Queue for an Interface, page 13-6). If this rule is for the global policy, then you need to manually add the priority queue to one or more interfaces before you configure the service policy rule.

Step 5
Select Enable policing, then check the Input policing or Output policing (or both) check boxes to enable the specified type of traffic policing. For each type of traffic policing, configure the following options:
- Committed Rate—The rate limit for this traffic flow; this is a value in the range 8000-2000000000, specifying the maximum speed (bits per second) allowed.
- Conform Action—The action to take when the rate is less than the conform-burst value. Values are transmit or drop.
- Exceed Action—Take this action when the rate is between the conform-rate value and the conform-burst value. Values are transmit or drop.
Monitor QoS

To monitor QoS in ASDM, you can enter commands at the Command Line Interface tool.

- QoS Police Statistics, page 13-8
- QoS Priority Statistics, page 13-8

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: TGL-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.
# 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 screens: Configuration &gt; Device Management &gt; Advanced &gt; Priority Queue Configuration &gt; Firewall &gt; Service Policy Rules.</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 modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules.</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>
Troubleshooting Connections and Resources

This chapter describes how to troubleshoot the ASA.

- Testing Your Configuration, page 14-1
- Monitoring Performance and System Resources, page 14-8
- Monitoring Connections, page 14-11

Testing Your Configuration

This section describes how to test connectivity for the single mode ASA or for each security context, how to ping the ASA interfaces, and how to allow hosts on one interface to ping through to hosts on another interface.

- Test Basic Connectivity: Pinging Addresses, page 14-1
- Trace Routes to Hosts, page 14-6
- Tracing Packets to Test Policy Configuration, page 14-8

Test Basic Connectivity: Pinging Addresses

Ping is a simple command that let’s you determine if a particular address is alive and responsive. The following topics explain more about the command and what types of testing you can accomplish with it.

- What You Can Test Using Ping, page 14-1
- Choosing Between ICMP and TCP Ping, page 14-2
- Enable ICMP, page 14-2
- Ping Hosts, page 14-3
- Test ASA Connectivity Systematically, page 14-4

What You Can Test Using Ping

When you ping a device, a packet is sent to the device and the device returns a reply. This process enables network devices to discover, identify, and test each other.
You can using ping to do the following tests:

- **Loopback testing of two interfaces**—You can initiate a ping from one interface to another on the same ASA, as an external loopback test to verify basic “up” status and operation of each interface.

- **Pinging to an ASA**—You can ping an interface on another ASA to verify that it is up and responding.

- **Pinging through an ASA**—You can ping through an intermediate ASA by pinging a device on the other side of the ASA. The packets will pass through two of the intermediate ASA’s interfaces as they go in each direction. This action performs a basic test of the interfaces, operation, and response time of the intermediate unit.

- **Pinging to test questionable operation of a network device**—You can ping from an ASA interface to a network device that you suspect is functioning incorrectly. If the interface is configured correctly and an echo is not received, there might be problems with the device.

- **Pinging to test intermediate communications**—You can ping from an ASA interface to a network device that is known to be functioning correctly. If the echo is received, the correct operation of any intermediate devices and physical connectivity is confirmed.

### Choosing Between ICMP and TCP Ping

The ASA includes the traditional ping, which sends ICMP Echo Request packets and gets Echo Reply packets in return. This is the standard tool and works well if all intervening network devices allow ICMP traffic. With ICMP ping, you can ping IPv4 or IPv6 addresses, or host names.

However, some networks prohibit ICMP. If this is true of your network, you can instead use TCP ping to test network connectivity. With TCP ping, the ping sends TCP SYN packets, and considers the ping a success if it receives a SYN-ACK in response. With TCP ping, you can ping IPv4 addresses or host names, but you cannot ping IPv6 addresses.

Keep in mind that a successful ICMP or TCP ping simply means that the address you are using is alive and responding to that specific type of traffic. This means that basic connectivity is working. Other policies running on a device could prevent specific types of traffic from successfully getting through a device.

### Enable ICMP

By default, you can ping from a high security interface to a low security interface. You just need to enable ICMP inspection to allow returning traffic through. If you want to ping from low to high, then you need to apply an ACL to allow traffic.

When pinging an ASA interface, any ICMP rules applied to the interface must allow Echo Request and Echo Response packets. ICMP rules are optional: if you do not configure them, all ICMP traffic to an interface is allowed.

This procedure explains all of ICMP configuration you might need to complete to enable ICMP pinging of ASA interfaces, or for pinging through an ASA.

### Procedure

**Step 1**

Ensure ICMP rules allow Echo Request/Echo Response.

ICMP rules are optional and apply to ICMP packets sent directly to an interface. If you do not apply ICMP rules, all ICMP access is allowed. In this case, no action is required.
However, if you do implement ICMP rules, ensure that you include rules that permit any address for the Echo and Echo-Reply messages on each interface. Configure ICMP rules on the Configuration > Device Management > Management Access > ICMP page.

**Step 2**  
Ensure access rules allow ICMP.

When pinging a host through an ASA, access rules must allow ICMP traffic to leave and return. The access rule must at least allow Echo Request/Echo Reply ICMP packets. You can add these rules as global rules.

If you do not have access rules, you will need to also allow the other type of traffic you want, because applying any access rules to an interface adds an implicit deny, so all other traffic will be dropped.

Configure access rules on the Configuration > Firewall > Access Rules page. If you are simply adding the rules for testing purposes, you can delete them after completing the tests.

**Step 3**  
Enable ICMP inspection.

ICMP inspection is needed when pinging through the ASA, as opposed to pinging an interface. Inspection allows returning traffic (that is, the Echo Reply packet) to return to the host that initiated the ping, and also ensures there is one response per packet, which prevents certain types of attack.

You can simply enable ICMP inspection in the default global inspection policy.


b. Edit the inspection_default global rule.

c. On the Rule Actions > Protocol Inspection tab, select ICMP.

d. Click OK, then Apply.

---

**Ping Hosts**

To ping any device, you simply choose Tools > Ping, enter the IP address or host name of the destination you are pinging, and click Ping. For TCP ping, you select TCP and also include the destination port. That is usually the extent of any test you need to run.

Example output for a successful ping:

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
???????
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If the ping fails, the output indicates ? for each failed attempt, and the success rate is less than 100 percent (complete failure is 0 percent):

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
???????
Success rate is 0 percent (0/5)
```

However, you can also add parameters to control some aspects of the ping. Following are your basic options:

- **ICMP ping**—You can select the interface through which the destination host is connected. If you do not select an interface, the routing table is used to determine the correct interface. You can ping IPv4 or IPv6 addresses or host names.

- **TCP ping**—You must also select the TCP port for the destination you are pinging. For example, **www.example.com 80** to ping the HTTP port. You can ping IPv4 addresses or host names, but not IPv6 addresses.
You also have the option to specify the source address and port that is sending the ping. In this case, optionally select the interface through which the source sends the ping (the routing table is used when you do not select an interface).

Finally, you can specify how often to repeat the ping (the default is 5 times) or the timeout for each attempt (the default is 2 seconds).

**Test ASA Connectivity Systematically**

If you want to do a more systematic test of ASA connectivity, you can use the following general procedure.

**Before You Begin**

If you want to see the syslog messages mentioned in the procedure, enable logging (the `logging enable` command, or Configuration > Device Management > Logging > Logging Setup in ASDM).

**Procedure**

**Step 1** Draw a diagram of your single-mode ASA or security context that shows the interface names, security levels, and IP addresses. The diagram should also include any directly connected routers and a host on the other side of the router from which you will ping the ASA.

**Figure 14-1  Network Diagram with Interfaces, Routers, and Hosts**

**Step 2** Ping each ASA interface from the directly connected routers. For transparent mode, ping the management IP address. This test ensures that the ASA interfaces are active and that the interface configuration is correct.
A ping might fail if the ASA interface is not active, the interface configuration is incorrect, or if a switch between the ASA and a router is down (see the following figure). In this case, no debugging messages or syslog messages appear, because the packet never reaches the ASA.

**Figure 14-2 Ping Failure at the ASA Interface**

If the ping reply does not return to the router, then a switch loop or redundant IP addresses might exist (see the following figure).

**Figure 14-3 Ping Failure Because of IP Addressing Problems**

**Step 3** Ping each ASA interface from a remote host. For transparent mode, ping the management IP address. This test checks whether the directly connected router can route the packet between the host and the ASA, and whether the ASA can correctly route the packet back to the host.

A ping might fail if the ASA does not have a return route to the host through the intermediate router (see the following figure). In this case, the debugging messages show that the ping was successful, but syslog message 110001 appears, indicating a routing failure has occurred.

**Figure 14-4 Ping Failure Because the ASA Has No Return Route**

**Step 4** Ping from an ASA interface to a network device that you know is functioning correctly.

- If the ping is not received, a problem with the transmitting hardware or interface configuration may exist.

- If the ASA interface is configured correctly and it does not receive an echo reply from the “known good” device, problems with the interface hardware receiving function may exist. If a different interface with “known good” receiving capability can receive an echo after pinging the same “known good” device, the hardware receiving problem of the first interface is confirmed.

**Step 5** Ping from the host or router through the source interface to another host or router on another interface. Repeat this step for as many interface pairs as you want to check. If you use NAT, this test shows that NAT is operating correctly.

If the ping succeeds, a syslog message appears to confirm the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter either the `show xlate` or `show conns` command to view this information.
The ping might fail because NAT is not configured correctly. In this case, a syslog message appears, showing that the NAT failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation, you get message 106010.

Figure 14-5 Ping Failure Because the ASA is Not Translating Addresses

---

Trace Routes to Hosts

If you are having problems sending traffic to an IP address, you can trace the route to the host to determine if there is a problem on the network path.

Procedure

Step 1 Make the ASA Visible on Trace Routes, page 14-6.

Make the ASA Visible on Trace Routes

By default, the ASA does not appear on traceroutes as a hop. To make it appear, you need to decrement the time-to-live on packets that pass through the ASA, and increase the rate limit on ICMP unreachable messages.

Procedure

Step 1 Decrement the TTL using a service policy.
   b. Add or edit a rule. For example, if you already have a rule to which you can add the option to decrement TTL, you do not need to create a new one.
   c. Progress through the wizard to the Rule Actions page, applying the rule globally or to an interface, and specifying the traffic match. For example, you could create a global match any rule.
   d. On the Rule Actions page, click the Connection Settings tab, and select Decrement time to live for a connection.
   e. Click OK or Finish, then Apply.
Step 2 Increase the ICMP unreachable rate limit.
   a. Choose Configuration > Device Management > Management Access > ICMP.
   b. Increase the IPv4 ICMP Unreachable Message Limits > Rate Limit value at the bottom of the page. For example, increase it to 50.
c. Click **Apply**.

---

### Determine Packet Routes

Use Traceroute to help you to determine the route that packets will take to their destination. A traceroute works by sending UDP packets to a destination on an invalid port. Because the port is not valid, the routers along the way to the destination respond with an ICMP Time Exceeded Message, and report that error to the ASA.

The traceroute shows the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following table explains the output symbols.

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

#### Procedure

**Step 1** Choose **Tools > Traceroute**.

**Step 2** Enter the destination hostname or IP address to which you are tracing the route. Configure a DNS server to use a host name.

**Step 3** (Optional) Configure the characteristics of the trace. The defaults are appropriate in most cases.

- **Timeout**—How long to wait for a response before timing out. The default is 3 seconds.
- **Port**—The UDP port to use. The default is 33434.
- **Probe**—How many probes to send at each TTL level. The default is 3.
- **TTL**—The minimum and maximum time-to-live values for the probes. The minimum default is one, but you can set it to a higher value to suppress the display of known hops. The maximum default is 30. The traceroute terminates when the packet reaches the destination or when the maximum value is reached.
- **Specify source interface or IP address**—The interface to use as the source of the trace. You can specify the interface by name or by IP address. In transparent mode, you must use the management address.
- **Reverse Resolve**—Whether to have the output display the names of hops encountered if DNS name resolution is configured. Deselect the option to show IP addresses only.
- **Use ICMP**—Whether to send ICMP probe packets instead of UDP probe packets.

**Step 4** Click **Trace Route** to start the traceroute.
Monitoring Performance and System Resources

You can monitor a variety of system resources to identify performance or other potential problems.

Tracing Packets to Test Policy Configuration

You can test your policy configuration by modeling a packet based on source and destination addressing and protocol characteristics. The trace does policy lookup to test access rules, NAT, routing, and so forth, to see if the packet would be permitted or denied.

By testing packets this way, you can see the results of your policies and test whether the types of traffic you want to allow or deny are handled as desired. Besides verifying your configuration, you can use the tracer to debug unexpected behavior, such as packets being denied when they should be allowed.

Procedure

- **Step 1** Choose **Tools > Packet Tracer**.
- **Step 2** Choose the source interface for the packet trace.
- **Step 3** Specify the protocol type for the packet trace. Available protocol types include ICMP, IP, TCP, and UDP.
- **Step 4** (Optional.) If you want to trace a packet where the security group tag value is embedded in the Layer 2 CMD header (Trustsec), check **SGT number** and enter the security group tag number, 0-65533.
- **Step 5** Specify the source and destination for the packets.
  - You can specify IPv4 or IPv6 addresses, fully-qualified domain names (FQDN), or security group names or tags, if you use Cisco Trustsec. For the source address, you can also specify a username in the format Domain\username.
- **Step 6** Specify the protocol characteristics:
  - ICMP—Enter the ICMP type, ICMP code (0-255), and optionally, the ICMP identifier.
  - TCP/UDP—Enter the source and destination port numbers.
  - Raw IP—Enter the protocol number, 0-255.
- **Step 7** Click **Start** to trace the packet.

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

The Traceroute Output area displays detailed messages about the traceroute results.

Monitoring Performance and System Resources

You can monitor a variety of system resources to identify performance or other potential problems.
Monitoring Performance

You can view ASA performance information in a graphical or tabular format.

Procedure

**Step 1** Choose Monitoring > Properties > Connection Graphs > Perfmon.

**Step 2** You can give the graph window a title by entering it in Graph Window Title, or you can choose an existing title.

**Step 3** Select up to four entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. The available options are the following:

- AAA Perfmon—Requests per second for authentication, authorization, and accounting requests.
- Inspection Perfmon—Packets per second for HTTP, FTP, and TCP inspection.
- Web Perfmon—Requests per second for URL access and URL server requests.
- Connections Perfmon—Connections per second for all connections, UDP connections, TCP connections, and TCP Intercept.
- Xlate Perfmon—NAT xlates per second.

**Step 4** Click Show Graphs.

You can toggle each graph between graph and table views. You can also change how often the data refreshes, and export or print the data.

Monitoring Memory Blocks

You can view free and used memory blocks information in a graphical or tabular format.

Procedure

**Step 1** Choose Monitoring > Properties > System Resources Graphs > Blocks.

**Step 2** You can give the graph window a title by entering it in Graph Window Title, or you can choose an existing title.

**Step 3** Select entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. The available options are the following:

- Blocks Used—Displays the ASA used memory blocks.
- Blocks Free—Displays the ASA free memory blocks.

**Step 4** Click Show Graphs.

You can toggle each graph between graph and table views. You can also change how often the data refreshes, and export or print the data.
Monitoring CPU

You can view CPU utilization.

**Procedure**

**Step 1** Choose Monitoring > Properties > System Resources Graphs > CPU.

**Step 2** You can give the graph window a title by entering it in Graph Window Title, or you can choose an existing title.

**Step 3** Add CPU Utilization to the Selected Graphs list.

**Step 4** Click Show Graphs.

You can toggle the graph between graph and table views. You can also change how often the data refreshes, and export or print the data.

Monitoring Memory

You can view memory utilization information in a graphical or tabular format.

**Procedure**

**Step 1** Choose Monitoring > Properties > System Resources Graphs > Memory.

**Step 2** You can give the graph window a title by entering it in Graph Window Title, or you can choose an existing title.

**Step 3** Select entries from the Available Graphs list, then click Add to move them to the Selected Graphs list. The available options are the following:

- Free Memory—Displays the ASA free memory.
- Used Memory—Displays the ASA used memory.

**Step 4** Click Show Graphs.

You can toggle each graph between graph and table views. You can also change how often the data refreshes, and export or print the data.
Monitoring Per-Process CPU Usage

You can monitor the processes that run on the CPU. You can obtain information about the percentage of CPU that is used by a certain process. CPU usage statistics are sorted in descending order to display the highest consumer at the top. Also included is information about the load on the CPU per process, at 5 seconds, 1 minute, and 5 minutes before the log time. This information is updated automatically every 5 seconds to provide real-time statistics. In ASDM, it is updated every 30 seconds.

To view CPU usage on a per-process basis, choose Monitoring > Properties > Per-Process CPU Usage.

You can stop the auto refresh, manually refresh the information, or save it to a file. You can also click the Configure CPU Usage Colors button to choose background and foreground colors based on usage percentages, to make it easier to scan for high-usage processes.

Monitoring Connections

To view current connections in a tabular format, in the ASDM main window, choose Monitoring > Properties > Connections. Information for each connection includes the protocol, source and destination address characteristics, idle time since the last packet was sent or received, and the amount of traffic in the connection.
PART 5

Advanced Network Protection
ASA and Cisco Cloud Web Security

Cisco Cloud Web Security (also known as ScanSafe) provides web security and web filtering services through the Software-as-a-Service (SaaS) model. Enterprises with the ASA in their network can use Cloud Web Security services without having to install additional hardware.

- Information About Cisco Cloud Web Security, page 15-1
- Licensing Requirements for Cisco Cloud Web Security, page 15-4
- Configure Cisco Cloud Web Security, page 15-6
- Examples for Cisco Cloud Web Security, page 15-16
- History for Cisco Cloud Web Security, page 15-21

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.

- Authentication Keys, page 15-2
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.

  For information about configuring IDFW, see the general operations configuration guide.

- **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, page 15-3
- Custom Groups, page 15-3
- How Groups and the Authentication Key Interoperate, page 15-4

**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.
  \`domain-name\group-name\`

  Note that on the ASA, the format is `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:
  
  `[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:
    \`domain-name\username\`
  - AAA usernames, when using RADIUS or TACACS+, are sent in the following format:
    \`LOCAL\username\`
  - AAA usernames, when using LDAP, are sent in the following format:
    \`domain-name\username\`
For the default username, it is sent in the following format:

\{domain-name\}username

For example, if you configure the default username to be “Guest,” then the ASA sends “Guest.” If you configure the default username to be “Cisco\Guest,” then the ASA sends “Cisco\Guest.”

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.

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 also 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 security appliance 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**

**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.

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

Before you configure Cloud Web Security, obtain a license and the addresses of the proxy servers you will use. Also, generate your authentication keys. Learn more about at Cloud Web Security http://www.cisco.com/go/cloudwebsecurity.

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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(Optional.) Configure the User Identity Monitor, page 15-14</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.
**Configure Cisco Cloud Web Security**

**Procedure**

**Step 1** Choose **Configuration > Device Management > Cloud Web Security**. In multiple context mode, do this in the system context.

![Configuration > Device Management > Cloud Web Security](image)

**Primary Server**
- IP Address/Domain Name: 192.168.43.10
- HTTP Port: 8080

**Backup Server**
- IP Address/Domain Name: server.example.com
- HTTP Port: 8080

**Other**
- Retry Counter: 5
- License Key: **************
- Confirm License Key: **************

**Step 2** Identify the primary and backup servers by IP address or fully-qualified domain name.

When you subscribe to the Cisco Cloud Web Security service, you are assigned primary and backup Cloud Web Security proxy servers.

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.

**Step 3** In the Other area, enter the following:
- Retry Counter—The number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable. Polls are performed every 30 seconds. Valid values are from 2 to 100, and the default is 5.
- License Key, Confirm License Key—The authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexadecimal number. It can be a company or group key.

**Step 4** Click **Apply**.

**Step 5** (Multiple context mode only.) Switch to each context where you want to use the service and enable it.

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.

---

**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** Choose Configuration > Firewall > Objects > Class Maps > Cloud Web Security.

**Step 2** Do one of the following:
- Click Add to add a new class map. Enter a map name, 40 characters or less, and optionally, a description.
- Select a map and click Edit.

**Step 3** Click Add to create a new class map.

The Add Cloud Web Security Traffic Class Map screen appears.

**Step 4** Choose a match option: Match All or Match Any.

**Match All** is the default, and specifies that traffic must match all criteria to match the class map. **Match Any** means that traffic matches the class map if it matches at least one criterion.

**Step 5** Configure the match criteria by adding or editing entries in the match table. Add as many as required to define the targeted traffic.

a. Choose the match type for the criteria: Match or No Match.
   - Match—Specifies the user or group that you want to whitelist.
   - No Match—Specifies the user or group that you do not want to whitelist; for example, if you whitelist the group “cisco,” but you want to scan traffic from users “johncrichton” and “aerynsun,” you can specify No Match for those users.

b. Choose whether you are defining a User, Group, or both, and enter the name of the user or group.

c. Click OK. Repeat the process until you add all your whitelist criteria.
Configure Cisco Cloud Web Security

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  Choose Configuration > Firewall > Service Policy, and open a rule.

- To create a new rule, click Add > Add Service Policy Rule. When adding a policy, you can apply it to a specific interface or globally to all interfaces. If there is already a global policy, or a policy for the interface, you are adding a rule to the existing policy. You can name new rules. Click Next to proceed.
Configure Cisco Cloud Web Security

Chapter 15  ASA and Cisco Cloud Web Security

If you have a ScanSafe inspection rule, or a rule to which you are adding ScanSafe inspection, select it and click Edit. Note that the “inspection_default” rule in the Global folder does not include the HTTP and HTTPS ports, so you cannot add ScanSafe inspection to that rule.

Step 2  On the Traffic Classification Criteria page, choose one of the following options to specify the traffic to which to apply the policy actions and click Next. When creating a new class, give the class a meaningful name. Also note that you must create separate classes for HTTP and HTTPS traffic.

- **Create a new traffic class > Source and Destination IP Address (uses ACL)**—If you do not already have a traffic class for Cloud Web Security, we recommend this option because ACL matching is the most flexible way to define the class.

  When you create a new traffic class of this type, you can only specify one access control entry (ACE) initially. After you finish adding the rule, you can add additional ACEs by adding a new rule to the same interface or global policy, and then specifying Add rule to existing traffic class.

- **Create a new traffic class > TCP or UDP Port**—Use this option if you do not want to differentiate among web traffic. When you click Next, specify one port, either TCP http or TCP https.

- **Add rule to existing traffic class**—If you have already started an ACL for Cisco Cloud Web Security inspection, and you are adding rules to the existing policy, select this option and select the traffic class.

Step 3  (ACL matching.) When defining the traffic class based on source and destination criteria, fill in the ACL attributes for this rule.

a. Click Match or Do Not Match.

  Match specifies that traffic matching the source and destination is sent to Cloud Web Security. Do Not Match exempts matching traffic from Cloud Web Security. You can later add additional rules to match or not match other traffic.

  When creating your rules, 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.

b. In the Source Criteria area, enter or browse for a Source IP address or network object. 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.

c. In the Destination Criteria area, enter or browse for a Destination IP address or network object, and an optional TrustSec Security Group.

  FQDN network objects might be useful in matching or exempting traffic to specific servers.

d. In the Service field, enter http or https, and click Next.
Cloud Web Security only operates on HTTP and HTTPS traffic. Each type of traffic is treated separately by the ASA. Therefore, you need to create HTTP-only rules and HTTPS-only rules.

**Step 4** On the Rule Actions page, Protocol Inspection tab, check the Cloud Web Security check box.

**Step 5** Click Configure to set the traffic action and add the inspection policy map.

The inspection policy map configures essential parameters for the rule and also optionally identifies the whitelist. An inspection policy map is required for each class of traffic that you want to send to Cloud Web Security. You can also pre-configure inspection policy maps by choosing Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security.

a. For the Cloud Web Security Traffic Action, choose one:
   - **Fail Close**—Drops all traffic if the Cloud Web Security servers are unavailable.
   - **Fail Open**—Allows traffic to pass through the ASA if the Cloud Web Security servers are unavailable.

b. Choose an existing inspection policy map, or click Add to add a new map.
c. (New maps only.) In the Cloud Web Security Inspection Map dialog box, enter a name for the map and configure the following attributes. Click OK when finished.

- **Default User and Group**—(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.

- **Protocol**—Select HTTP or HTTPS based on the service you selected in the traffic class. These selections must match. Cloud Web Security treats each type of traffic separately.
• **Inspections** tab—(Optional) To identify a whitelist, click the **Add** on the Inspections tab and select the class map for the whitelist. You can also add a whitelist at this time by clicking **Manage**. Ensure that **Whitelist** is selected as the action and click **OK**. You can add additional whitelists.

d. Click **OK** in the Select Cloud Web Security Inspect Map dialog box.

**Step 6**

Click **Finish**. The rule is added to the Service Policy Rules table.

**Step 7**

To add additional sub-rules (ACEs) for this traffic class, to match or exempt additional traffic, repeat the process, selecting the same interface or global policy. When you configure the traffic class, select the option to **Add rule to existing traffic class**, and select the Cloud Web Security class.

When you configure the new ACE, ensure that you specify the same service used by the other rules in the class, either HTTP or HTTPS.

Do not make changes to the Rule Actions page. Click **Finish** when the rule is complete.
Step 8  Repeat this entire procedure to create traffic class for the other protocol, for example for HTTPS traffic (assuming you started with an HTTP traffic class). You can create as many rules and sub-rules as needed.

Step 9  Arrange the order of Cloud Web Security rules and sub-rules on the Service Policy Rules pane. Select the rule you want to move and click the up or down buttons. Ensure that specific rules come before more general rules.

Step 10  Click Apply.

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** Choose Configuration > Firewall > Identity Options, and scroll to the Cloud Web Security Configuration section.

**Step 2** Click Add.

**Step 3** Select the domain that includes the group, then double-click the group in the user groups list and click OK to add it. Repeat the process to add more groups.

- If there are a large number of groups, use the Find box to filter the list. The ASA downloads names from AD for the specified domain.
- You can also type in a group name directly in the format `domain_name\group_name`.
- If necessary, you can add new domains by clicking the Manage button.

**Step 4** After you add all the groups you want to monitor, click Apply.

---

**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](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, select Monitoring > Properties > Cloud Web Security. This page shows the proxy server status and statistics for redirected HTTP/HTTPS connections. In multiple context mode, statistics are only shown within a context.

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](http://Whoami.scansafe.net)
Examples for Cisco Cloud Web Security

Following are some examples for configuring Cloud Web Security.

- Example Service Policy for Cloud Web Security, page 15-16

Example Service Policy for Cloud Web Security

The following example exempts all IPv4 HTTP and HTTPS traffic going to the 10.6.6.0/24 network, sends all other HTTPS and HTTPS traffic to Cloud Web Security, and applies this service policy rule to all interfaces as part of the existing global policy. If the Cloud Web Security server is unreachable, the ASA drops all matching traffic (fail close). If a user does not have user identity information, the default user Boulder and group Cisco is used.

**Step 1** Choose Configuration > Firewall > Service Policy Rules, and click Add > Service Policy Rule. Add this rule to the default global_policy. Click Next.

**Step 2** Add a new traffic class called “scansafe-http,” and specify an ACL for traffic matching. Click Next.
Step 3  Choose **Match**, and specify **any4** for the Source and Destination. Specify **tcp/http** for the Service. Click **Next**.

Step 4  Check **Cloud Web Security** on the Protocol Inspection tab and click **Configure**.

Step 5  Accept the default Fail Close action, and click **Add**.
Step 6  Name the inspection policy map “http-map,” set the Default User to Boulder and the default group to Cisco. Choose HTTP.

Step 7  Click OK, OK, and then Finish. The rule is added to the Service Policy Rules table.
Step 8  Choose Configuration > Firewall > Service Policy Rules, and click Add > Service Policy Rule. Add the new rule to the default global_policy and click Next.

Step 9  Click Add rule to existing traffic class, and choose scansafe-http.

Step 10 Choose Do not match, set any4 as the Source, and 10.6.6.0/24 as the Destination. Set the Service to tcp/http. Click Next.
Step 11  Click **Finish**.

Step 12  Reorder the rules so the Do not match rule is above the Match rule.

User traffic is compared to these rules in order; if this Match rule is first in the list, then all traffic, including traffic to the test network, will match only that rule and the Do not match rule will never be hit. If you move the Do not match rule above the Match rule, then traffic to the test network will match the Do not match rule, and all other traffic will match the Match rule.

Step 13  Repeat the above steps with the following changes: add a new traffic class called “scansafe-https,” and choose **HTTPS** for the inspection policy map.
History for Cisco Cloud Web Security

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Cloud Web Security    | 9.0(1)            | 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 screens:  
Configuration > Device Management > Cloud Web Security  
Configuration > Firewall > Objects > Class Maps > Cloud Web Security  
Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security  
Configuration > Firewall > Identity Options  
Configuration > Firewall > Service Policy Rules  
Monitoring > Properties > Cloud Web Security |
Threat Detection

This chapter describes how to configure threat detection statistics and scanning threat detection.

- Detecting Threats, page 16-1
- Guidelines for Threat Detection, page 16-3
- Defaults for Threat Detection, page 16-4
- Configure Threat Detection, page 16-4
- Monitoring Threat Detection, page 16-6
- History for Threat Detection, page 16-7

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 no data UDP session 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>

Caution

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.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

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 in Tools > Command Line Interface.

For advanced statistics, by default, statistics for ACLs are enabled.

### Table 16-2 Basic Threat Detection Default Settings

<table>
<thead>
<tr>
<th>Packet Drop Reason</th>
<th>Trigger Settings</th>
<th>Average Rate</th>
<th>Burst Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>· DoS attack detected</td>
<td>100 drops/sec over the last 600 seconds.</td>
<td>400 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td>· Bad packet format</td>
<td>80 drops/sec over the last 3600 seconds.</td>
<td>320 drops/sec over the last 120 second period.</td>
<td></td>
</tr>
<tr>
<td>· Connection limits exceeded</td>
<td>100 drops/sec over the last 600 seconds.</td>
<td>200 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td>· Suspicious ICMP packets detected</td>
<td>80 drops/sec over the last 3600 seconds.</td>
<td>160 drops/sec over the last 120 second period.</td>
<td></td>
</tr>
<tr>
<td>Scanning attack detected</td>
<td>5 drops/sec over the last 600 seconds.</td>
<td>10 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td>Incomplete session detected such as TCP SYN attack detected or no data UDP session attack detected (combined)</td>
<td>100 drops/sec over the last 600 seconds.</td>
<td>200 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td>Denial by ACLs</td>
<td>80 drops/sec over the last 3600 seconds.</td>
<td>160 drops/sec over the last 120 second period.</td>
<td></td>
</tr>
<tr>
<td>· Basic firewall checks failed</td>
<td>400 drops/sec over the last 600 seconds.</td>
<td>800 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td>· Packets failed application inspection</td>
<td>320 drops/sec over the last 3600 seconds.</td>
<td>640 drops/sec over the last 120 second period.</td>
<td></td>
</tr>
<tr>
<td>Interface overload</td>
<td>2000 drops/sec over the last 600 seconds.</td>
<td>8000 drops/sec over the last 20 second period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1600 drops/sec over the last 3600 seconds.</td>
<td>6400 drops/sec over the last 120 second period.</td>
<td></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.
Chapter 16  Threat Detection

Configure Threat Detection

Procedure

Step 1  Configure Basic Threat Detection Statistics, page 16-5.
Basic threat detection statistics include activity that might be related to an attack, such as a DoS attack.


Step 3  Configure Scanning Threat Detection, page 16-6.

Configure Basic Threat Detection Statistics

Basic threat detection statistics is enabled by default. You can disabled it, or turn it on again if you disable it.

Procedure

Step 1  Choose the Configuration > Firewall > Threat Detection.
Step 2  Select or deselect Enable Basic Threat Detection as desired.
Step 3  Click Apply.

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  Choose Configuration > Firewall > Threat Detection.
Step 2  In the Scanning Threat Statistics area, choose one of the following options:
  •  Enable All Statistics.
  •  Disable All Statistics.
  •  Enable Only Following Statistics.
Step 3  If you chose Enable Only Following Statistics, then select one or more of the following options:
  •  Hosts—Enables host statistics. The host statistics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
  •  Access Rules (enabled by default)—Enables statistics for access rules.
  •  Port—Enables statistics for TCP and UDP ports.
  •  Protocol—Enables statistics for non-TCP/UDP IP protocols.
**Configure Scanning Threat Detection**

You can configure scanning threat detection to identify attackers and optionally shun them.

**Procedure**

**Step 1** Choose **Configuration > Firewall > Threat Detection**.

**Step 2** Select **Enable Scanning Threat Detection**.

**Step 3** (Optional) To automatically terminate a host connection when the ASA identifies the host as an attacker, select **Shun Hosts detected by scanning threat** and fill in these options if desired:

- To exempt host IP addresses from being shunned, enter an address or the name of a network object in the **Networks excluded from shun** field. You can enter multiple addresses or subnets separated by commas. To choose a network from the list of IP address objects, click the ... button.

- To set the duration of a shun for an attacking host, select **Set Shun Duration** and enter a value between 10 and 2592000 seconds. The default length is 3600 seconds (1 hour). To restore the default value, click **Set Default**.

**Step 4** Click **Apply**.

---

**Monitoring Threat Detection**

The following topics explain how to monitor threat detection and view traffic statistics.

- **Monitoring Basic Threat Detection Statistics, page 16-7**

---

**TCP-Intercept**—Enables statistics for attacks intercepted by TCP Intercept (to enable TCP Intercept, see **Protect Servers from a SYN Flood DoS Attack (TCP Intercept), page 12-4**).

**Step 4** For host, port, and protocol statistics, you can change the number of rate intervals collected. In the Rate Intervals area, choose **1 hour, 1 and 8 hours, or 1, 8 and 24 hours** for each statistics type. The default interval is **1 hour**, which keeps the memory usage low.

**Step 5** For TCP Intercept statistics, you can set the following options in the TCP Intercept Threat Detection area:

- **Monitoring Window Size**—Sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. 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.

- **Burst Threshold 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 Threshold 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.

Click **Set Default** to restore the default values.

**Step 6** Click **Apply**.
Monitoring Basic Threat Detection Statistics

Choose **Home > Firewall Dashboard > Traffic Overview** to view basic threat detection statistics.

Monitoring Advanced Threat Detection Statistics

You can monitor advanced threat statistics using the following dashboards:

- **Home > Firewall Dashboard > Top 10 Access Rules**—Displays the most hit access rules. Permits and denies are not differentiated in this graph. You can track denied traffic in the Traffic Overview > Dropped Packets Rate graph.

- **Home > Firewall Dashboard > Top Usage Statistics**—The Top 10 Sources and Top 10 Destinations tabs show statistics for hosts. Due to the threat detection algorithm, an interface used as a combination failover and state link could appear in the top 10 hosts; this is expected behavior, and you can ignore this IP address in the display.

  The Top 10 Services tab shows statistics for both ports and protocols (both must be enabled for the display), and shows the combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.

- **Home > Firewall Dashboard > Top Ten Protected Servers under SYN Attack**—Shows the TCP Intercept statistics. Click the Detail button to show 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 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 screens were introduced: Configuration &gt; Firewall &gt; Threat Detection, Home &gt; Firewall Dashboard &gt; Traffic Overview, Home &gt; Firewall Dashboard &gt; Top 10 Access Rules, Home &gt; Firewall Dashboard &gt; Top Usage Status, Home &gt; Firewall Dashboard &gt; Top 10 Protected Servers Under SYN Attack.</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 screens was modified: Configuration &gt; Firewall &gt; Threat Detection.</td>
</tr>
</tbody>
</table>
### History for Threat Detection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Intercept statistics</td>
<td>8.0(4)/8.1(2)</td>
<td>TCP Intercept statistics were introduced. The following screens were introduced or modified: Configuration &gt; Firewall &gt; Threat Detection, Home &gt; Firewall Dashboard &gt; Top 10 Protected Servers Under SYN Attack.</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 screen was modified: Configuration &gt; Firewall &gt; Threat Detection.</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>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 screen was modified: Configuration &gt; Firewall &gt; Threat Detection.</td>
</tr>
<tr>
<td>Improved memory usage</td>
<td>8.3(1)</td>
<td>The memory usage for threat detection was improved.</td>
</tr>
</tbody>
</table>

---

**Platform**

- **Releases**
  - 8.0(4)/8.1(2)
  - 8.1(2)
  - 8.2(1)
  - 8.3(1)

**Description**

- TCP Intercept statistics were introduced.
- 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.
- 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.
- 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 memory usage for threat detection was improved.
PART 6

ASA Modules
ASA FirePOWER (SFR) Module

This chapter describes how to configure the ASA FirePOWER module that runs on the ASA.

- The ASA FirePOWER Module, page 16-1
- Licensing Requirements for the ASA FirePOWER Module, page 16-6
- Guidelines for ASA FirePOWER, page 16-6
- Defaults for ASA FirePOWER, page 16-7
- Configure the ASA FirePOWER Module, page 16-7
- Managing the ASA FirePOWER Module, page 16-21
- Monitoring the ASA FirePOWER Module, page 16-26
- History for the ASA FirePOWER Module, page 16-28

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). You can use the module in single or multiple context mode, and in routed or transparent mode.

The module is also known as ASA SFR.

Although the module has a basic command line interface (CLI) for initial configuration and troubleshooting, you configure the security policy on the device using a separate application, FireSIGHT Management Center, which can be hosted on a separate FireSIGHT Management Center appliance or as a virtual appliance running on a VMware server. (FireSIGHT Management Center is also known as Defense Center.)

For ASA FirePOWER running on ASA 5506-X devices, you can optionally configure the device using ASDM rather than FireSIGHT Management Center.

- How the ASA FirePOWER Module Works with the ASA, page 16-1
- ASA FirePOWER Management Access, page 16-5
- Compatibility with ASA Features, page 16-6

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.
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.

You cannot configure both inline tap monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed. In multiple context mode, you cannot configure inline tap monitor-only mode for some contexts, and regular inline mode for others.

The following figure shows the traffic flow when operating in inline tap mode.
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 Access

There are two separate layers of access for managing an ASA FirePOWER module: initial configuration (and subsequent troubleshooting) and policy management.

- Initial Configuration, page 16-5
- Policy Configuration and Management, page 16-5

Initial Configuration

For initial configuration, you must use the CLI on the ASA FirePOWER module. For information on the default management addresses, see Defaults for ASA FirePOWER, page 16-7.

To access the CLI, you can use the following methods:

- ASA 5585-X (hardware module):
  - ASA FirePOWER console port—The console port on the module is a separate external console port.
  - ASA FirePOWER Management 1/0 interface using SSH—you can connect to the default IP address or you can use ASDM to change the management IP address and then connect using SSH. The management interface on the module is a separate external Gigabit Ethernet interface.

  **Note** You cannot access the ASA FirePOWER hardware module CLI over the ASA backplane using the session command.

- All other models (software module):
  - ASA session over the backplane—if you have CLI access to the ASA, then you can session to the module and access the module CLI.
  - ASA FirePOWER Management 0/0 interface using SSH (Management 1/1 for the 5506-X)—You can connect to the default IP address or you can use ASDM to change the management IP address and then connect using SSH. The ASA FirePOWER management interface shares the management interface with the ASA. Separate MAC addresses and IP addresses are supported for the ASA and ASA FirePOWER module. You must perform configuration of the ASA FirePOWER IP address within the ASA FirePOWER operating system (using the CLI or ASDM). However, physical characteristics (such as enabling the interface) are configured on the ASA. You can remove the ASA interface configuration (specifically the interface name) to dedicate this interface as an ASA FirePOWER-only interface. This interface is management-only.

Policy Configuration and Management

After you perform initial configuration, configure the ASA FirePOWER security policy using FireSIGHT Management Center (for all models) or ASDM (for 5506-X). Then configure the ASA policy for sending traffic to the ASA FirePOWER module using ASDM or Cisco Security Manager.
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.

To take full advantage of the ASA FirePOWER module features, use the following guidelines for traffic that you send to the ASA FirePOWER module:

- Do not configure ASA inspection on HTTP traffic.
- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both ASA FirePOWER inspection and Cloud Web Security inspection for the same traffic, the ASA only performs ASA FirePOWER inspection.
- Other application inspections on the ASA are compatible with the ASA FirePOWER module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA FirePOWER module.

Licensing Requirements for the ASA FirePOWER Module

The ASA FirePOWER module and FireSIGHT Management Center require additional licenses, which need to be installed in the module itself rather than in the context of the ASA. The ASA itself requires no additional licenses.

See the Licensing chapter of the FireSIGHT System User Guide or the online help in FireSIGHT Management Center for more information.

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 (using FireSIGHT Management Center) to ensure consistent failover behavior.

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 using FireSIGHT Management Center. Do not use different ASA-interface-based zone definitions for devices in the cluster.

Model Guidelines

- For ASA model software and hardware compatibility with the ASA FirePOWER module, see Cisco ASA Compatibility.
For the 5512-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 5506-X.)

Additional Guidelines and Limitations
- See Compatibility with ASA Features, page 16-6.
- You cannot change the software type installed on the hardware module; if you purchase an ASA FirePOWER module, you cannot later install other software on it.
- You cannot configure both normal inline mode and inline tap monitor-only mode at the same time on the ASA. Only one type of security policy 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 16-1 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: 192.168.8.24</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: Sourcefire</td>
</tr>
<tr>
<td></td>
<td>• Boot image: Admin123</td>
</tr>
</tbody>
</table>

Configure the ASA FirePOWER Module

Configuring the ASA FirePOWER module is a process that includes configuration of the ASA FirePOWER security policy on the ASA FirePOWER module and then configuration of the ASA to send traffic to the ASA FirePOWER module. To configure the ASA FirePOWER module, perform the following steps:

**Step 1** Connect the ASA FirePOWER Management Interface, page 16-8. Cable the ASA FirePOWER management interfaces and optionally, the console interface.

**Step 2** (If necessary.) Install or Reimage the Software Module, page 16-11. Skip this step if you purchased a model with the software module pre-installed.

**Step 3** (If necessary.) Change the ASA FirePOWER Management IP Address, page 16-14. This might be required for initial SSH access.

**Step 4** Configure Basic ASA FirePOWER Settings at the ASA FirePOWER CLI, page 16-15. You do this on the ASA FirePOWER module.

**Step 5** (Optional for ASA 5506-X.) Add ASA FirePOWER to the FireSIGHT Management Center, page 16-16. This identifies the FireSIGHT Management Center that will manage the device. If you do not configure a FireSIGHT Management Center for the 5506-X, you can manage the module using ASDM.
Connect the ASA FirePOWER Management Interface

In addition to providing management access to the ASA FirePOWER module, the ASA FirePOWER management interface needs access to an HTTP proxy server or a DNS server and the Internet for signature updates and more. This section describes recommended network configurations. Your network may differ.

ASA 5585-X (Hardware Module)

The ASA FirePOWER module includes a separate management and console interface from the ASA. For initial setup, you can connect with SSH to the ASA FirePOWER Management 1/0 interface using the default IP address. If you cannot use the default IP address, you can either use the console port or use ASDM to change the management IP address so you can use SSH. (See Change the ASA FirePOWER Management IP Address, page 16-14.)

If you have an inside router

If you have an inside router, you can route between the management network, which can include both the ASA Management 0/0 and ASA FirePOWER Management 1/0 interfaces, and the ASA inside network for Internet access. Be sure to also add a route on the ASA to reach the Management network through the inside router.
If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network, which would require an inside router to route between the networks. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. Because the ASA FirePOWER module is a separate device from the ASA, you can configure the ASA FirePOWER Management 1/0 address to be on the same network as the inside interface.

ASA 5506-X and 5512-X through ASA 5555-X (Software Module)

These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER management interface shares the Management 0/0 interface with the ASA (Management 1/1 on 5506-X). For initial setup, you can connect with SSH to the ASA FirePOWER default IP address. If you cannot use the default IP address, you can either session to the ASA FirePOWER over the backplane or use ASDM to change the management IP address so you can use SSH.
If you have an inside router

If you have an inside router, you can route between the Management 0/0 or 1/1 network, which includes both the ASA and ASA FirePOWER management IP addresses, and the inside network for Internet access. Be sure to also add a route on the ASA to reach the Management network through the inside router.

If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 or 1/1 interface. If you remove the ASA-configured name from the Management 0/0 or 1/1 interface, you can still configure the ASA FirePOWER IP address for that interface. Because the ASA FirePOWER module is essentially a separate device from the ASA, you can configure the ASA FirePOWER management address to be on the same network as the inside interface.

Note

You must remove the ASA-configured name for Management 0/0 or 1/1; if it is configured on the ASA, then the ASA FirePOWER address must be on the same network as the ASA, and that excludes any networks already configured on other ASA interfaces. If the name is not configured, then the ASA FirePOWER address can be on any network, for example, the ASA inside network.
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 device 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.

  hostname# sw-module module ips shutdown
  hostname# sw-module module ips uninstall
  hostname# reload

- 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.

- When reimaging the module, use the same shutdown and uninstall commands to remove the old image. For example, sw-module module sfr uninstall.

- Obtain both the ASA FirePOWER Boot Image and System Software packages from Cisco.com.

Procedure

**Step 1** Download the boot image to the device. 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://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img disk0:/asasfr-5500x-boot-5.3.1-58.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; replace <TFTP Server> with your server's IP address or host name.

  ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
  disk0:/asasfr-5500x-boot-5.3.1-58.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.
Configure the ASA FirePOWER Module

Chapter 16  ASA FirePOWER (SFR) Module

Step 3  Set the ASA FirePOWER module boot image location in ASA disk0 by entering the following command:

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

If you get 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.

Example:

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

Step 4  Load the ASA FirePOWER boot image by entering the following command:

```
hostname# 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  Use the `setup` command to configure the system so that you can install the system software package.

```
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 using the `system install` command:

```
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. Allow 10 or more minutes for application component installation and for the ASA FirePOWER services to start. (The `show module sfr` output should show all processes as Up.)
For example:

```
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
  Description:                    Cisco ASA-FirePOWER 5.3.1-44 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.
```
asa3# session sfr console
```
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is ‘CTRL-~X’.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:

**Step 9** Log in with the username **admin** and the password **Sourcefire**.

**Step 10** Complete the system configuration as prompted.

You must first read and accept the end user license agreement (EULA). Then change the admin password, then configure the management address and DNS settings, as prompted. You can configure both IPv4 and IPv6 management addresses. For 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 an IPV4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
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 11** (Optional for 5506-X.) Identify the FireSIGHT Management Center appliance that will manage this device using the `configure manager add` command.

You come up with a registration key, which you will then use in FireSIGHT Management Center when you add the device to its inventory. The following example shows the simple case. When there is a NAT boundary, the command is different; see Add ASA FirePOWER to the FireSIGHT Management Center, page 16-16.

```bash
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

For the 5506-X, you can instead use ASDM to configure the policy on the ASA FirePOWER module. When using ASDM, you can configure one module at a time, which is a good solution when you have a single device or very few devices. If you have a large number of devices, FireSIGHT Management Center is a better solution.

**Step 12** (Skip for 5506-X when using ASDM.) Log into the FireSIGHT Management Center using an HTTPS connection in a browser, using the hostname or address entered above. For example, https://DC.example.com.

Use the Device Management (**Devices > Device Management**) page to add the device. For more information, see the online help or the Managing Devices chapter in the FireSIGHT System User Guide.

**Tip**

You also configure NTP and time settings through FireSIGHT Management Center. Use the Time Synchronization settings when editing the local policy from the **System > Local > System Policy** page.

---

### Change the ASA FirePOWER Management IP Address

If you cannot use the default management IP address, then you can set the management IP address from the ASA. After you set the management IP address, you can access the ASA FirePOWER module using SSH to perform additional setup.

If you already configured the management address during initial system setup through the ASA FirePOWER CLI, as described in Configure Basic ASA FirePOWER Settings at the ASA FirePOWER CLI, page 16-15, then it is not necessary to configure it through the ASA CLI or ASDM.

**Note**

For a software module, you can access the ASA FirePOWER CLI to perform setup by sessioning from the ASA CLI; you can then set the ASA FirePOWER management IP address as part of setup. For a hardware module, you can complete the initial setup through the Console port.
To change the management IP address through the ASA, do one of the following. In multiple context mode, perform this procedure in the system execution space.

- In the CLI, use the following command to set the ASA FirePOWER management IP address, mask, and gateway. Use \(1\) for a hardware module, \(sfr\) for a software module.

\[
\text{session} \ (1 \ | \ sfr) \ \text{do} \ \text{setup} \ \text{host} \ \text{ip} \ \text{ip\_address/mask,gateway\_ip}
\]

For example, \(\text{session} \ 1 \ \text{do} \ \text{setup} \ \text{host} \ \text{ip} \ 10.1.1.2/24,10.1.1.1\).

- In ASDM, choose Wizards > Startup Wizard, and progress through the wizard to the ASA FirePOWER Basic Configuration, where you can set the IP address, mask, and default gateway.

### Configure Basic ASA FirePOWER Settings at the ASA FirePOWER CLI

You must configure basic network settings and other parameters on the ASA FirePOWER module before you can configure your security policy. This procedure assumes you have the full system software installed (not just the boot image), either after you installed it directly, or because it is already installed on a hardware module.

**Tip**

This procedure also assumes that you are performing an initial configuration. During initial configuration, you are prompted for these settings. If you need to change these settings later, use the various `configure network` commands to change the individual settings. For more information on the `configure network` commands, use the `?` command for help, and see the FireSIGHT System User Guide, or the online help in FireSIGHT Management Center.

**Procedure**

**Step 1**

Do one of the following:

- (All models.) Use SSH to connect to the ASA FirePOWER management IP address.
- (Software modules only.) Open a session to the module from the ASA CLI (see the “Getting Started” chapter in the general operations configuration guide to access the ASA CLI). In multiple context mode, session from the system execution space.

```
hostname# session sfr
```

**Step 2**

Log in with the username `admin` and the password `Sourcefire`.

**Step 3**

Complete the system configuration as prompted.

You must first read and accept the end user license agreement (EULA). Then change the admin password, then configure the management address and DNS settings, as prompted. You can configure both IPv4 and IPv6 management addresses. The configuration is complete when you see the message that says the sensor must be managed by a FireSIGHT Management Center.

For 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]:
```
Configure the ASA FirePOWER Module

Enter an IPv4 address for the management interface [192.168.45.45]: \textbf{10.86.118.3}

Enter an IPv4 netmask for the management interface [255.255.255.0]: \textbf{255.255.252.0}

Enter the IPv4 default gateway for this system [10.86.116.1]: \textbf{10.86.118.3}

Enter a fully qualified hostname for this system [Sourcefire3D]: \textbf{asasfr.example.com}

Enter a comma-separated list of DNS servers or 'none' []: \textbf{10.100.10.15, 10.120.10.14}

Enter a comma-separated list of search domains or 'none' [example.net]: \textbf{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.

\textbf{Step 4} (Optional for 5506-X.) Now you must identify the FireSIGHT Management Center that will manage this device, as explained in Add ASA FirePOWER to the FireSIGHT Management Center, page 16-16.

\section*{Add ASA FirePOWER to the FireSIGHT Management Center}

FireSIGHT Management Center, also known as Defense Center, is a separate server that manages multiple FirePOWER devices for the same or different models. FireSIGHT Management Center is ideal for managing large deployments, providing configuration consistency across your devices and efficiency in traffic analysis.

For ASA 5512-X through 5585-X, you must register the module to a FireSIGHT Management Center. There is no other way to configure the module.

To register a device, use the \texttt{configure manager add} command. A unique alphanumeric registration key is always required to register a device to a FireSIGHT Management Center. This is a simple key that you specify, and is not the same as a license key.

In most cases, you must provide the FireSIGHT Management Center’s hostname or the IP address along with the registration key, for example:

\texttt{configure manager add DC.example.com my_reg_key}

However, if the device and the FireSIGHT Management Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

\texttt{configure manager add DONTRESOLVE my_reg_key my_nat_id}
Configure the ASA FirePOWER Module

Configure the ASA FirePOWER Module

The security policy controls the services provided by the module, such as Next Generation IPS filtering and application filtering.

You use FireSIGHT Management Center to configure the security policy on the module.

For the ASA 5506-X, you can alternatively use ASDM. However, you can never use both ASDM and FireSIGHT Management Center, you must choose one or the other. If you configure a FireSIGHT Management Center for the module, you must use the configured manager. If you do not configure a manager, you must use ASDM.

There is no CLI for configuring the security policy.
Configure the ASA FirePOWER Module

Chapter 16  ASA FirePOWER (SFR) Module

Configure the Security Policy with FireSIGHT Management Center

To open FireSIGHT Management Center, do one of the following:

- 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 Add ASA FirePOWER to the FireSIGHT Management Center, page 16-16. For example, https://dc.example.com.
- In ASDM, choose Home > ASA FirePOWER Status and click the link at the bottom of the
  dashboard.

For information about how to configure the security policy, see the FireSIGHT System User Guide or the
online help in FireSIGHT Management Center.

Configure the Security Policy with ASDM

For ASA 5506-X, if you do not configure a FireSIGHT Management Center, you use ASDM to configure
the security policy.

ASA FirePOWER pages are separate from the ASA configuration pages. Use the following pages to
monitor and configure the module. You can click Help in any page, or choose Help > ASA FirePOWER
Help Topics, to learn more about how to configure policies.

- Home > ASA FirePOWER Dashboard—The dashboard provides summary information about the
  software running on the module, product updates, licensing, system load, disk usage, system time,
  and interface status.
- Home > ASA FirePOWER Reporting—The reporting page provides Top 10 dashboards for a wide
  variety of module statistics, such as web categories, users, sources, and destinations for the traffic
  passing through the module.
- Home > ASA FirePOWER Status—Also available when you manage the module with FireSIGHT
  Management Center, the status page includes module information, such as the model, serial number,
  and software version, and module status, such as the application name and status, data plane status,
  and overall status. If the module is registered to a FireSIGHT Management Center, you can click the
  link to open the application and do further analysis and module configuration.
- Configuration > ASA FirePOWER Configuration—This drawer includes pages for each ASA
  FirePOWER policy, such as access control and intrusion policies. The configuration of these
  policies is consistent with the same policies in FireSIGHT Management Center, so you can easily
  transition between the two products. Click Help within the policy page to get detailed information
  on configuring the policies.
- Configuration > Firewall > Access Rules—When you choose to configure ASA FirePOWER with
  ASDM, the ASA access rules page includes toggle buttons so that you can easily switch the view
  between ASA rules and ASA FirePOWER rules. Keep in mind that ASA inbound rules on an
  interface are always applied before ASA FirePOWER access control policies. Any traffic dropped
  through inbound rules is never sent to ASA FirePOWER.
- Monitoring > ASA FirePOWER Monitoring—There are several pages for monitoring the module,
  including syslog, task status, module statistics, and a real-time event viewer.
ASDM Restrictions for Managing ASA FirePOWER

Keep the following restrictions in mind when configuring ASA FirePOWER using ASDM.

- 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 configure the ASA in a failover pair, the ASA FirePOWER configuration is not automatically synchronized with the ASA FirePOWER module on the secondary device. Thus, you must manually export the ASA FirePOWER configuration from the primary and import it into the secondary every time you make a change. We recommend using FireSIGHT Management Center for any device configured for failover.

- If you are using Java 7_u51 up to Java 8, you need to import the SSL certificate from the ASA FirePOWER module to your workstation to view the configuration pages. Go to Wizard > ASDM Identity Certificate Wizard to obtain the certificate. Then, go to your Java Control Panel and import it, and restart ASDM. This is a general issue with these Java versions, and you will also need to import the certificate from the ASA to configure it through ASDM.

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 the 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. 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 Choose Configuration > Firewall > Service Policy Rules.
Step 2 Choose Add > Add Service Policy Rule.
Step 3 Choose whether to apply the policy to a particular interface or apply it globally and click Next.
Configure the ASA FirePOWER Module

Step 4 Configure the traffic match. For example, you could match Any Traffic so that all traffic that passes your inbound access rules is redirected to the module. Or, you could define stricter criteria based on ports, ACL (source and destination criteria), or an existing traffic class. The other options are less useful for this policy. After you complete the traffic class definition, click Next.

Step 5 On the Rule Actions page, click the ASA FirePOWER Inspection tab.

Step 6 Check the Enable ASA FirePOWER for this traffic flow check box.

Step 7 In the If ASA FirePOWER Card Fails area, click one of the following:
- Permit traffic—Sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
- Close traffic—Sets the ASA to block all traffic if the module is unavailable.

Step 8 (Optional) Check Monitor-only to send a read-only copy of traffic to the module, i.e. inline tap mode. By default, the traffic is sent in inline mode. Be sure to configure consistent policies on the ASA and the ASA FirePOWER. Both policies should reflect the inline or monitor-only of the traffic.

Step 9 Click Finish and then Apply.
Repeat this procedure to configure additional traffic flows as desired.

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, page 16-4.

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.

**Examples**

The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
    no nameif
    traffic-forward sfr monitor-only
    no shutdown
```

---

**Managing the ASA FirePOWER Module**

This section includes procedures that help you manage the module.

- Reset the Password, page 16-21
- Reload or Reset the Module, page 16-22
- Shut Down the Module, page 16-22
- Uninstall a Software Module Image, page 16-22
- Session to the Software Module From the ASA, page 16-23
- Reimage the 5585-X ASA FirePOWER Hardware Module, page 16-23
- Upgrade the System Software, page 16-25

---

**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 using the `session do` command.

**Tip**

The password-reset option on the ASA hw-module and sw-module commands does not work with ASA FirePOWER.
To reset the module password for the user **admin** to the default, **Sourcefire**, use the following command. Use **1** for a hardware module, **sfr** for a software module. In multiple context mode, perform this procedure in the system execution space.

```
session (1 | sfr) do password-reset
```

For example, **session sfr do password-reset**.

### Reload or Reset the Module

To reload, or to reset and then reload, the module, enter one of the following commands at the ASA CLI. In multiple context mode, perform this procedure in the system execution space.

- **Hardware module (ASA 5585-X):**
  ```
  hw-module module 1 {reload | reset}
  ```

- **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. To gracefully shut down the module, enter one of the following commands at the ASA CLI. In multiple context mode, perform this procedure in the system execution space.

- **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. In multiple context mode, perform this procedure in the system execution space.

#### Procedure

**Step 1** Uninstall the software module image and associated configuration.

```
hostname# 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. You must reload the ASA before you can install a new module.

```
hostname# reload
```

---

**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 is `Sourcefire` for the full image, and `Admin123` for the boot image.

- **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.

---

**Reimage the 5585-X ASA FirePOWER Hardware Module**

If you need to reimage the ASA FirePOWER hardware module in an ASA 5585-X appliance 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.

To accomplish a TFTP boot, you must:

- Place the software image on a TFTP server that can be accessed through the Management1/0 interface on the ASA FirePOWER.
- Connect Management1/0 to the network. You must use this interface to TFTP boot the Boot Image.
- Configure rommon variables. Press Esc to interrupt the auto-boot process so that you can configure rommon variables.

Once the boot image is installed, you install the System Software package. You must place the package on an HTTP, HTTPS, or FTP server that is accessible from the ASA FirePOWER.

The following procedure explains how to install the boot image and then install the System Software package.

**Procedure**

**Step 1** Connect to the Console port. Use the console cable included with the ASA product to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your ASA for more information about the console cable.

**Step 2** Enter the `system reboot` command to reload the system.

**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` and 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`.

For example:

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

**Step 5** Enter `sync` to save the settings.

**Step 6** Enter `tftp` to initiate the download and boot process.

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** Use the `setup` command to configure the system so that you can install the system software package.
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 using the `system install` command:

```
  system install [noconfirm] url
```

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.

For example:

```
  asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.3.1-54.pkg
```

**Step 10**

When the boot completes, log in as `admin` with the password `Sourcefire`.

Complete the system configuration as prompted.

You must first read and accept the end user license agreement (EULA). Then change the admin password, then configure the management address and DNS settings, as prompted. You can configure both IPv4 and IPv6 management addresses.

**Step 11**

Identify the FireSIGHT Management Center appliance that will manage this device using the `configure manager add` command.

You come up with a registration key, which you will then use in FireSIGHT Management Center when you add the device to its inventory. The following example shows the simple case. When there is a NAT boundary, the command is different; see Add ASA FirePOWER to the FireSIGHT Management Center, page 16-16.

```
  > configure manager add 10.89.133.202 123456
  Manager successfully configured.
```

**Step 12**

Log into the FireSIGHT Management Center using an HTTPS connection in a browser, using the hostname or address entered above. For example, `https://DC.example.com`.

Use the Device Management (Devices > Device Management) page to add the device. For more information, see the Managing Devices chapter in the FireSIGHT System User Guide or the online help in FireSIGHT Management Center.

---

**Upgrade the System Software**

Use FireSIGHT Management Center to apply upgrade images to the ASA FirePOWER module. 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 FireSIGHT System User Guide or the online help in FireSIGHT Management Center.
If you are managing the module through ASDM, 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.

Use Tools > Command Line Interface to use monitoring commands.
- Showing Module Status, page 16-26
- Showing Module Statistics, page 16-26
- Analyzing Operational Behavior (5506-X Only), page 16-27
- Monitoring Module Connections, page 16-27

### Showing Module Status

From the Home page, you can select the ASA FirePOWER Status tab to view information about the module. This includes module information, such as the model, serial number, and software version, and module status, such as the application name and status, data plane status, and overall status. If the module is registered to a FireSIGHT Management Center, you can click the link to open the application and do further analysis and module configuration.

For 5506-X, when managing the module with ASDM, you can also use the Home > ASA FirePOWER Dashboard page to view summary information about the software running on the module, product updates, licensing, system load, disk usage, system time, and interface status.

### 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
Analyzing Operational Behavior (5506-X Only)

When you manage the 5506-X ASA FirePOWER module using ASDM rather than FireSIGHT Management Center, you can view operational information for the module using these pages:

- **Home > ASA FirePOWER Reporting**—The reporting page provides Top 10 dashboards for a wide variety of module statistics, such as web categories, users, sources, and destinations for the traffic passing through the module.
- **Monitoring > ASA FirePOWER Monitoring**—There are several pages for monitoring the module, including syslog, task status, module statistics, and a real-time event viewer.

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'.

### 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 the following screens: Home &gt; ASA FirePOWER Status Wizards &gt; Startup Wizard &gt; ASA FirePOWER Basic Configuration Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA FirePOWER Inspection</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) 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. We introduced the following screens: Home &gt; ASA FirePOWER Dashboard, Home &gt; ASA FirePOWER Reporting, Configuration &gt; ASA FirePOWER Configuration (including sub-pages), Monitoring &gt; ASA FirePOWER Monitoring (including sub-pages).</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: <strong>traffic-forward sfr monitor-only</strong>. You can configure this in CLI only.</td>
</tr>
</tbody>
</table>
ASA CX Module

This chapter describes how to configure the ASA CX module that runs on the ASA.

- The ASA CX Module, page 18-1
- Licensing Requirements for the ASA CX Module, page 18-6
- Prerequisites for ASA CX, page 18-6
- Guidelines for ASA CX, page 18-6
- Defaults for ASA CX, page 18-8
- Configure the ASA CX Module, page 18-8
- Managing the ASA CX Module, page 18-19
- Monitoring the ASA CX Module, page 18-21
- Troubleshooting Problems with the Authentication Proxy, page 18-23
- History for the ASA CX Module, page 18-24

The ASA CX Module

The ASA CX module lets you enforce security based on the full context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook, or permitting finance employees access to a sensitive enterprise database but denying the same access to other employees.

- How the ASA CX Module Works with the ASA, page 18-2
- ASA CX Management Access, page 18-4
- Authentication Proxy for Active Authentication, page 18-5
- Compatibility with ASA Features, page 18-5
How the ASA CX Module Works with the ASA

The ASA CX module runs a separate application from the ASA. The module can be a hardware module (on the ASA 5585-X) or a software module (5512-X through 5555-X). As a hardware module, the device includes separate management and console ports, and extra data interfaces that are used directly by the ASA and not by the module itself.

You can configure your device in either a normal inline mode or in monitor-only mode for demonstration purposes.

- In an inline deployment, the actual traffic is sent to the device, and the device’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.
- In a monitor-only deployment, a copy of the traffic is sent to the device, but it is not returned to the ASA. Monitor-only mode lets you see what the device would have done to traffic without impacting the network. You can configure this mode using a monitor-only service policy or a traffic forwarding interface. For guidelines and limitations for monitor-only mode, see Guidelines for ASA CX, page 18-6.

The following sections explain these modes in more detail.

ASA CX Normal Inline Mode

In normal inline mode, traffic goes through the firewall checks before being forwarded to the ASA CX module. When you identify traffic for ASA CX inspection on the ASA, traffic flows through the ASA and the ASA CX 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 CX module.
5. The ASA CX module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA CX 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 CX module. In this example, the ASA CX module automatically blocks traffic that is not allowed for a certain application. All other traffic is forwarded through the ASA.
Service Policy in Monitor-Only Mode

For testing and demonstration purposes, you can configure the ASA to send a duplicate stream of read-only traffic to the ASA CX module, so you can see how the module inspects the traffic without affecting the ASA traffic flow. In this mode, the ASA CX module inspects the traffic as usual, makes policy decisions, and generates events. However, because the packets are read-only copies, the module actions do not affect the actual traffic. Instead, the module drops the copies after inspection. The following figure shows the ASA CX module in monitor-only mode.

Traffic-Forwarding Interface in Monitor-Only Mode

You can alternatively configure ASA interfaces to be traffic-forwarding interfaces, where all traffic received is forwarded directly to the ASA CX module without any ASA processing. For testing and demonstration purposes, traffic-forwarding removes the extra complication of ASA processing. Traffic-forwarding is only supported in monitor-only mode, so the ASA CX module drops the traffic after inspecting it. The following figure shows the ASA GigabitEthernet 0/3 interface configured for traffic-forwarding. That interface is connected to a switch SPAN port so the ASA CX module can inspect all of the network traffic.
ASA CX Management Access

There are two separate layers of access for managing an ASA CX module: initial configuration (and subsequent troubleshooting) and policy management.

- Initial Configuration, page 18-4
- Policy Configuration and Management, page 18-5

Initial Configuration

For initial configuration, you must use the CLI on the ASA CX module to run the **setup** command and configure other optional settings.

To access the CLI, you can use the following methods:

- **ASA 5585-X:**
  - ASA CX console port—The ASA CX console port is a separate external console port.
  - ASA CX Management 1/0 interface using SSH—You can connect to the default IP address (192.168.8.8), or you can use ASDM to change the management IP address and then connect using SSH. The ASA CX management interface is a separate external Gigabit Ethernet interface.

  **Note** You cannot access the ASA CX hardware module CLI over the ASA backplane using the **session** command.

- **ASA 5512-X through ASA 5555-X:**
  - ASA session over the backplane—If you have CLI access to the ASA, then you can session to the module and access the module CLI.
  - ASA CX Management 0/0 interface using SSH—You can connect to the default IP address (192.168.1.2), or you can use ASDM to change the management IP address and then connect using SSH. These models run the ASA CX module as a software module. The ASA CX management interface shares the Management 0/0 interface with the ASA. Separate MAC addresses and IP addresses are supported for the ASA and ASA CX module. You must perform
configuration of the ASA CX IP address within the ASA CX operating system (using the CLI or ASDM). However, physical characteristics (such as enabling the interface) are configured on the ASA. You can remove the ASA interface configuration (specifically the interface name) to dedicate this interface as an ASA CX-only interface. This interface is management-only.

**Policy Configuration and Management**

After you perform initial configuration, configure the ASA CX policy using Cisco Prime Security Manager (PRSM). PRSM is both the name of the ASA CX configuration interface and the name of a separate product for configuring ASA CX devices, Cisco Prime Security Manager.

Then configure the ASA policy for sending traffic to the ASA CX module using ASDM, the ASA CLI, or PRSM in multiple-device mode.

**Authentication Proxy for Active Authentication**

You can configure identity policies on the ASA CX to collect user identity information for use in access policies. The system can collect user identity either actively (by prompting for username and password credentials) or passively (by retrieving information collected by AD Agent or Cisco Context Directory Agent, CDA).

If you want to use active authentication, you must configure the ASA to act as an authentication proxy. The ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. The default port is 885, but you can configure a different port.

To enable active authentication, you enable the authentication proxy as part of the service policy that redirects traffic to ASA CX, as explained in Create the ASA CX Service Policy, page 18-17.

**Compatibility with ASA Features**

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA CX module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

To take full advantage of the ASA CX module features, see the following guidelines for traffic that you send to the ASA CX module:

- Do not configure ASA inspection on HTTP traffic.
- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both the ASA CX action and Cloud Web Security inspection for the same traffic, the ASA only performs the ASA CX action.
- Other application inspections on the ASA are compatible with the ASA CX module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA CX module.
- Do not enable ASA clustering; it is not compatible with the ASA CX module.
Licensing Requirements for the ASA CX Module

The ASA CX module and PRSM require additional licenses, which need to be installed in the module itself rather than in the context of the ASA. The ASA itself requires no additional licenses. See the ASA CX documentation for more information.

Prerequisites for ASA CX

To use PRSM to configure the ASA, you need to install a certificate on the ASA for secure communications. By default, the ASA generates a self-signed certificate. However, this certificate can cause browser prompts asking you to verify the certificate because the publisher is unknown. To avoid these browser prompts, you can instead install a certificate from a known certificate authority (CA). If you request a certificate from a CA, be sure the certificate type is both a server authentication certificate and a client authentication certificate. See the general operations configuration guide for more information.

Guidelines for ASA CX

Context Mode Guidelines
Starting with ASA CX 9.1(3), multiple context mode is supported.

However, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy. Therefore, you cannot use the same IP addresses in multiple contexts; each context must include unique networks.

Firewall Mode Guidelines
Supported in routed and transparent firewall mode. Traffic-forwarding interfaces are only supported in transparent mode.

Failover Guidelines
Does not support failover directly; when the ASA fails over, any existing ASA CX flows are transferred to the new ASA, but the traffic is allowed through the ASA without being inspected by the ASA CX. Only new flows received by the new ASA are acted upon by the ASA CX module.

ASA Clustering Guidelines
Does not support clustering.

IPv6 Guidelines
- Supports IPv6.
- (9.1(1) and earlier) Does not support NAT 64. In 9.1(2) and later, NAT 64 is supported.

Model Guidelines
- Supported only on the ASA 5585-X and 5512-X through ASA 5555-X. See the Cisco ASA Compatibility Matrix for more information:
For the 5512-X through ASA 5555-X, you must install a Cisco solid state drive (SSD). For more information, see the ASA 5500-X hardware guide.

**Monitor-Only Mode Guidelines**

Monitor-only mode is strictly for demonstration purposes and is not a normal operational mode for the module.

- You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed. In multiple context mode, you cannot configure monitor-only mode for some contexts, and regular inline mode for others.
- The following features are not supported in monitor-only mode:
  - Deny policies
  - Active authentication
  - Decryption policies
- The ASA CX does not perform packet buffering in monitor-only mode, and events will be generated on a best-effort basis. For example, some events, such as ones with long URLs spanning packet boundaries, may be impacted by the lack of buffering.
- Be sure to configure both the ASA policy and the ASA CX to have matching modes: both in monitor-only mode, or both in normal inline mode.

Additional guidelines for traffic-forwarding interfaces:

- The ASA must be in 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 CX traffic.

**Additional Guidelines and Limitations**

- See Compatibility with ASA Features, page 18-5.
- You cannot change the software type installed on the hardware module; if you purchase an ASA CX module, you cannot later install other software on it.
Defaults for ASA CX

The following table lists the default settings for the ASA CX module.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>ASA 5585-X: Management 1/0 192.168.8.8/24</td>
</tr>
<tr>
<td></td>
<td>ASA 5512-X through ASA 5555-X: Management 0/0 192.168.1.2/24</td>
</tr>
<tr>
<td>Gateway</td>
<td>ASA 5585-X: 192.168.8.1/24</td>
</tr>
<tr>
<td></td>
<td>ASA 5512-X through ASA 5555-X: 192.168.1.1/24</td>
</tr>
<tr>
<td>SSH or session Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>Admin123</td>
</tr>
</tbody>
</table>

Configure the ASA CX Module

Configuring the ASA CX module is a process that includes configuration of the ASA CX security policy on the ASA CX module and then configuration of the ASA to send traffic to the ASA CX module. To configure the ASA CX module, perform the following steps:

Step 1  Connect the ASA CX Management Interface, page 18-9. Cable the ASA CX management interfaces and optionally, the console interface.

Step 2  (ASA 5512-X through ASA 5555-X) Install or Reimage the Software Module, page 18-11.

Step 3  (ASA 5585-X) Change the ASA CX Management IP Address, page 18-14, if necessary. This might be required for initial SSH access.

Step 4  Configure Basic ASA CX Settings, page 18-14. You do this on the ASA CX module.


Step 6  (Optional.) Configure the Authentication Proxy Port, page 18-16

Step 7  Redirect Traffic to the ASA CX Module, page 18-16.
Connect the ASA CX Management Interface

In addition to providing management access to the ASA CX module, the ASA CX management interface needs access to an HTTP proxy server or a DNS server and the Internet for signature updates and more. This section describes recommended network configurations. Your network may differ.

ASA 5585-X (Hardware Module)

The ASA CX module includes a separate management and console interface from the ASA. For initial setup, you can connect with SSH to the ASA CX Management 1/0 interface using the default IP address (192.168.8.8/24). If you cannot use the default IP address, you can either use the console port or use ASDM to change the management IP address so you can use SSH.

If you have an inside router

If you have an inside router, you can route between the management network, which can include both the ASA Management 0/0 and ASA CX Management 1/0 interfaces, and the ASA inside network for Internet access. Be sure to also add a route on the ASA to reach the Management network through the inside router.
If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network, which would require an inside router to route between the networks. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. Because the ASA CX module is a separate device from the ASA, you can configure the ASA CX Management 1/0 address to be on the same network as the inside interface.

**ASA 5512-X through ASA 5555-X (Software Module)**

These models run the ASA CX module as a software module, and the ASA CX management interface shares the Management 0/0 interface with the ASA. For initial setup, you can connect with SSH to the ASA CX default IP address (192.168.1.2/24). If you cannot use the default IP address, you can either session to the ASA CX over the backplane or use ASDM to change the management IP address so you can use SSH.
If you have an inside router

If you have an inside router, you can route between the Management 0/0 network, which includes both the ASA and ASA CX management IP addresses, and the inside network for Internet access. Be sure to also add a route on the ASA to reach the Management network through the inside router.

If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. If you remove the ASA-configured name from the Management 0/0 interface, you can still configure the ASA CX address for that interface. Because the ASA CX module is essentially a separate device from the ASA, you can configure the ASA CX management address to be on the same network as the inside interface.

Note

You must remove the ASA-configured name for Management 0/0; if it is configured on the ASA, then the ASA CX address must be on the same network as the ASA, and that excludes any networks already configured on other ASA interfaces. If the name is not configured, then the ASA CX address can be on any network, for example, the ASA inside network.

(ASA 5512-X through ASA 5555-X) Install or Reimage the Software Module

If you purchase the ASA with the ASA CX module, the module software and required solid state drives (SSDs) come pre-installed and ready to go. If you want to add the ASA CX to an existing ASA, or need to replace the SSD, you need to install the ASA CX boot software and partition the SSD according to this procedure. To physically install the SSD, see the ASA hardware guide.
Reimaging the module is the same procedure, except you should first uninstall the ASA CX module. You would reimagine a system if you replace an SSD.

**Note**
For the ASA 5585-X hardware module, you must install or upgrade your image from within the ASA CX module. See the ASA CX module documentation for more information.

**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 device 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.

  ```
  hostname# sw-module module ips shutdown
  hostname# sw-module module ips uninstall
  hostname# reload
  ```

  **Note** If you have an active service policy redirecting traffic to an IPS module, you must remove that policy. For example, if the policy is a global one, you would use `no service-policy ips_policy global`. You can remove the policies using CLI or ASDM.

- When reimaging the module, use the same shutdown and uninstall commands to remove the old image. For example, `sw-module module cxsc uninstall`.

**Procedure**

**Step 1** Download the boot image to the device. 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://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.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; replace `<TFTP Server>` with your server’s IP address or host name.

  ```
  ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.img
  ```

**Step 2** Download the ASA CX system software from Cisco.com to an HTTP, HTTPS, or FTP server accessible from the ASA CX management interface.

**Step 3** Set the ASA CX module boot image location in ASA disk0 by entering the following command:

  ```
  hostname# sw-module module cxsc recover configure image disk0:file_path
  ```
Chapter 18      ASA CX Module

Configure the ASA CX Module

Note
If you get a message like “ERROR: Another service (ips) 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.

Example:
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img

Step 4 Load the ASA CX boot image by entering the following command:
hostname# sw-module module cxsc recover boot

Step 5 Wait approximately 5 minutes for the ASA CX module to boot up, and then open a console session to the now-running ASA CX boot image. The default username is admin and the default password is Admin123.
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123

Tip
If the module boot has not competed, the session command will fail with a message about not being able to connect over ttyS1. Wait and try again.

Step 6 Partition the SSD:
asacx-boot> partition
....
Partition Successfully Completed

Step 7 Perform the basic network setup using the setup command according to Configure Basic ASA CX Settings, page 18-14 (do not exit the ASA CX CLI), and then return to this procedure to install the software image.

Step 8 Install the System Software image using the system install command:
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, which closes the console session. Allow 10 or more minutes for application component installation and for the ASA CX services to start. (The show module cxsc output should show all processes as Up.)
The following command installs the asacx-sys-9.3.1.1-112.pkg system software.
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg
Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
(ASA 5585-X) Change the ASA CX Management IP Address

If you cannot use the default management IP address (192.168.8.8), then you can set the management IP address from the ASA. After you set the management IP address, you can access the ASA CX module using SSH to perform initial setup.

For a software module, you can access the ASA CX CLI to perform setup by sessioning from the ASA CLI; you can then set the ASA CX management IP address as part of setup. See Configure Basic ASA CX Settings, page 18-14.

To change the management IP address through the ASA, do one of the following. In multiple context mode, perform this procedure in the system execution space.

- In the CLI, use the following command to set the ASA CX management IP address, mask, and gateway.
  
  ```
  session 1 do setup host ip ip_address/mask, gateway_ip
  ```

  For example, `session 1 do setup host ip 10.1.1.2/24,10.1.1.1`.

- (Single context mode only.) In ASDM, choose Wizards > Startup Wizard, and progress through the wizard to the ASA CX Basic Configuration, where you can set the IP address, mask, and default gateway. You can also set a different authentication proxy port if the default does not suit you.

Configure Basic ASA CX Settings

You must configure basic network settings and other parameters on the ASA CX module before you can configure your security policy. The ASA CX CLI is the only method for configuring these settings.

Procedure

Step 1

Do one of the following:

- (All models) Use SSH to connect to the ASA CX management IP address.
- (ASA 5512-X through ASA 5555-X) Open a console session to the module from the ASA CLI. In multiple context mode, session from the system execution space.
  
  ```
  hostname# session cxsc console
  ```
Step 2  Log in with the username *admin* and the password *Admin123*. You will change the password as part of this procedure.

Step 3  Enter the following command:

```
asacx> setup
```

**Example:**

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

You are prompted through the setup wizard. The following example shows a typical path through the wizard; if you enter *Y* instead of *N* at a prompt, you will be able to configure some additional settings. This example shows how to configure both IPv4 and IPv6 static addresses. You can configure IPv6 stateless auto configuration by answering *N* when asked if you want to configure a static IPv6 address.

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

Step 4  After you complete the final prompt, you are presented with a summary of the settings. Look over the summary to verify that the values are correct, and enter *Y* to apply your changed configuration. Enter *N* to cancel your changes.

**Example:**

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

---

**Note**  If you change the host name, the prompt does not show the new name until you log out and log back in.

---

Step 5  If you do not use NTP, configure the time settings. The default time zone is the UTC time zone. Use the `show time` command to see the current settings. You can use the following commands to change time settings:

```
asacx> config timezone
asacx> config time
```
Step 6  Change the admin password by entering the following command:

```
asacx> config passwd
```

Example:

```
asacx> config passwd
The password must be at least 8 characters long and must contain at least one uppercase letter (A-Z), at least one lowercase letter (a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

Step 7  Enter the `exit` command to log out.

---

**Configure the Security Policy on the ASA CX Module**

You use PRSM to configure the security policy on the ASA CX module. The security policy controls the services provided by the module. You cannot configure the policy through the ASA CX CLI, the ASA CLI, or ASDM.

PRSM is both the name of the ASA CX configuration interface and the name of a separate product for configuring ASA CX devices, Cisco Prime Security Manager. The method for accessing the configuration interface, and how to use it, are the same. For details on using PRSM to configure your ASA CX security policy, see the ASA CX/PRSM user guide or online help.

To open PRSM, use a web browser to open the following URL:

```
https://management_address
```

Where `management_address` is the DNS name or IP address of the ASA CX management interface or the PRSM server. For example, `https://asacx.example.com`.

There is a shortcut to this address on Home > ASA CX Status; click the Connect to the ASA CX application link to open the ASA CX or PRSM server that is managing the module.

---

**Configure the Authentication Proxy Port**

If you use active authentication in ASA CX policies, the ASA uses port 885 as the authentication proxy port. You can configure a different port if 885 is not acceptable, but a non-default port must be higher than 1024. For more information about the authentication proxy, see Authentication Proxy for Active Authentication, page 18-5.

In multiple context mode, change the port within each security context.

To change the authentication proxy port, choose Configuration > Firewall > Advanced > ASA CX Auth Proxy. You can also set the port as part of the ASDM startup wizard.

---

**Redirect Traffic to the ASA CX Module**

You can redirect traffic to the ASA CX module by creating a service policy that identifies specific traffic. For demonstration purposes only, you can also enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected.
Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA.

- Create the ASA CX Service Policy, page 18-17
- Configure Traffic-Forwarding Interfaces (Monitor-Only Mode), page 18-18

### Create the ASA CX Service Policy

You redirect traffic to the ASA CX module by creating a service policy that identifies specific traffic.

**Note**

ASA CX redirection is bidirectional. Thus, if you configure the service policy for one interface, and there is a connection between hosts on that interface and an interface for which redirection is not configured, then all traffic between these hosts is sent to the ASA CX module, including traffic originating on the non-ASA CX interface. However, the ASA only performs the authentication proxy on the interface to which the service policy is applied, because authentication proxy is applied only to ingress traffic.

**Before You Begin**

- If you enable the authentication proxy on the ASA using this procedure, be sure to also configure a directory realm for authentication on the ASA CX module. See the ASA CX user guide for more information.
- If you have an active service policy redirecting traffic to an IPS module (that you replaced with the ASA CX), you must remove that policy before you configure the ASA CX service policy.
- Be sure to configure both the ASA policy and the ASA CX to have matching modes: both in monitor-only mode, or both in normal inline mode.
- In multiple context mode, perform this procedure within each security context.
- When using PRSM in multiple device mode, you can configure the ASA policy for sending traffic to the ASA CX module within PRSM, instead of using ASDM or the ASA CLI as explained below. However, PRSM has some limitations when configuring the ASA service policy; see the ASA CX user guide for more information.

**Procedure**

3. Complete the Service Policy dialog box as desired. See the ASDM online help for more information about these screens.
5. Complete the Traffic Classification Criteria dialog box as desired. See the ASDM online help for more information about these screens.
6. Click Next to show the Add Service Policy Rule Wizard - Rule Actions dialog box.
7. Click the ASA CX Inspection tab.
8. Check the Enable ASA CX for this traffic flow check box.
Step 9  In the If ASA CX Card Fails area, choose one of the following:
  • **Permit traffic**—Sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
  • **Close traffic**—Sets the ASA to block all traffic if the module is unavailable.

Step 10 To enable the authentication proxy, which is required for active authentication, check the **Enable Auth Proxy** check box. This option is not available in monitor-only mode.

Step 11 (Optional) For demonstration purposes only, check the **Monitor-only** check box to send a read-only copy of traffic to the ASA CX module.

**Note**  You must configure all classes and policies to be either in monitor-only mode, or in normal inline mode; you cannot mix both modes on the same ASA.

Step 12  Click **Finish** and then **Apply**.
Repeat this procedure to configure additional traffic flows as desired.

### Configure Traffic-Forwarding Interfaces (Monitor-Only Mode)

For demonstration purposes only, you can configure traffic-forwarding interfaces, where all traffic is forwarded directly to the ASA CX module. For normal ASA CX operation, see Create the ASA CX Service Policy, page 18-17.

For more information, see Traffic-Forwarding Interface in Monitor-Only Mode, page 18-3. See also Guidelines for ASA CX, page 18-6 for guidelines and limitations specific to traffic-forwarding interfaces.

You can only configure this feature at the CLI. Choose **Tools > Command Line Interface**, then click the **Multiple Line** radio button, and enter the commands. Click **Send** when the command block is complete.

**Before You Begin**
  • Be sure to configure both the ASA policy and the ASA CX to have matching modes: both in monitor-only.
  • In multiple context mode, perform this procedure within each security context.

**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 cxsc monitor-only
```
Step 4 Enable the interface.

no shutdown

Repeat for any additional interfaces.

Examples
The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward cxsc monitor-only
  no shutdown
```

Managing the ASA CX Module

This section includes procedures that help you manage the module.

- Reset the Password, page 18-19
- Reload or Reset the Module, page 18-20
- Shut Down the Module, page 18-20
- (ASA 5512-X through ASA 5555-X) Uninstall a Software Module Image, page 18-20
- (ASA 5512-X through ASA 5555-X) Session to the Module From the ASA, page 18-21

Reset the Password

You can reset the module password to the default. For the user admin, the default password is Admin123. After resetting the password, you should change it to a unique value using the module application.

Resetting the module password causes the module to reboot. Services are not available while the module is rebooting.

To reset the module password to the default, use one of the following techniques. In multiple context mode, perform this procedure in the system execution space.

- (CLI) Hardware module (ASA 5585-X):
  hw-module module 1 password-reset
- (CLI) Software module (ASA 5512-X through ASA 5555-X):
  sw-module module cxsc password-reset
- (ASDM) Choose Tools > ASA CX Password Reset.

Note If you cannot connect to ASDM with the new password, restart ASDM and try to log in again. If you defined a new password and still have an existing password in ASDM that is different from the new password, clear the password cache by choosing File > Clear ASDM Password Cache, then restart ASDM and try to log in again.
### Reload or Reset the Module

To reload, or to reset and then reload, the module, enter one of the following commands at the ASA CLI. In multiple context mode, perform this procedure in the system execution space.

- Hardware module (ASA 5585-X):
  
  ```
  hw-module module 1 {reload | reset}
  ```

- Software module (ASA 5512-X through ASA 5555-X):
  
  ```
  sw-module module cxsc {reload | reset}
  ```

### Shut Down the Module

Shutting down the module software prepares the module to be safely powered off without losing configuration data. To gracefully shut down the module, enter one of the following commands at the ASA CLI. In multiple context mode, perform this procedure in the system execution space.

---

**Note**

If you reload the ASA, the module is not automatically shut down, so we recommend shutting down the module before reloading the ASA.

- Hardware module (ASA 5585-X):
  
  ```
  hw-module module 1 shutdown
  ```

- Software module (ASA 5512-X through ASA 5555-X):
  
  ```
  sw-module module cxsc shutdown
  ```

### (ASA 5512-X through ASA 5555-X) Uninstall a Software Module Image

You can uninstall a software module image and its associated configuration. In multiple context mode, perform this procedure in the system execution space.

#### Procedure

1. **Step 1** Uninstall the software module image and associated configuration.

   ```
   hostname# sw-module module cxsc uninstall
   ```

   Module cxsc will be uninstalled. This will completely remove the disk image associated with the sw-module including any configuration that existed within it.

   Uninstall module cxsc? [confirm]

2. **Step 2** Reload the ASA. You must reload the ASA before you can install a new module.

   ```
   hostname# reload
   ```
(ASA 5512-X through ASA 5555-X) Session to the Module From the ASA

Use the ASA CX CLI to configure basic network settings and to troubleshoot the module.

To access the ASA CX software module CLI from the ASA, you can session from the ASA. 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. Use the admin username and password (default is Admin123).

- Telnet session:
  ```
  session cxsc
  ```
  When in the ASA CX CLI, to exit back to the ASA CLI, use the exit command, or press Ctrl-Shift-6, x.

- Console session:
  ```
  session cxsc 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 cxsc 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 CX console and return to the ASA prompt. Therefore, if you try to exit the ASA CX 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 CX 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 cxsc command instead of the console command when facing this situation.

Monitoring the ASA CX Module

The following topics provide guidance on monitoring the module. For ASA CX-related syslog messages, see the syslog messages guide. ASA CX syslog messages start with message number 429001.

Use Tools > Command Line Interface to use monitoring commands.

- Showing Module Status, page 18-21
- Showing Module Statistics, page 18-22
- Monitoring Module Connections, page 18-22

Showing Module Status

From the Home page, you can select the ASA CX Status tab to view information about the module. This includes module information, such as the model, serial number, and software version, and module status, such as the application name and status, data plane status, and overall status. You can click the link to open the application and do further analysis and module configuration.
Showing Module Statistics

Use the `show service-policy cxsc` command to display statistics and status for each service policy that includes the `cxsc` command. Use `clear service-policy` to clear the counters.

The following is sample output from the `show service-policy` command showing the ASA CX policy and the current statistics as well as the module status when the authentication proxy is disabled:

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

The following is sample output from the `show service-policy` command showing the ASA CX policy and the current statistics as well as the module status when the authentication proxy is enabled; in this case, the proxied counters also increment:

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

Monitoring Module Connections

To show connections through the ASA CX module, enter one of the following commands:

- **show asp table classify domain cxsc**
  
  Shows the NP rules created to send traffic to the ASA CX module.

- **show asp table classify domain cxsc-auth-proxy**
  
  Shows the NP rules created for the authentication proxy for the ASA CX module. In the following is sample output, which shows one rule, the destination "port=2000" is the auth-proxy port configured by the `cxsc auth-proxy port 2000` command, and the destination “ip/id=192.168.0.100” is the ASA interface IP address.

```
hostname# show asp table classify domain cxsc-auth-proxy
Input Table
  in id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0
  dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
  input_ifc=inside, output_ifc=identity
```

- **show asp drop**
  
  Shows dropped packets. The drop types are explained below.

- **show asp event dp-cp cxsc-msg**
  
  This output shows how many ASA CX module messages are on the dp-cp queue. Only VPN queries from the ASA CX module are sent to dp-cp.
• **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 CX module.

**Frame Drops:**
- **cxsc-bad-tlv-received**—This occurs when ASA receives a packet from CXSC 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.
- **cxsc-request**—The frame was requested to be dropped by CXSC due a policy on CXSC whereby CXSC would set the actions to Deny Source, Deny Destination, or Deny Pkt.
- **cxsc-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).
- **cxsc-fail**—The CXSC configuration was removed for an existing flow and we are not able to process it through CXSC; it will be dropped. This should be very unlikely.
- **cxsc-malformed-packet**—The packet from CXSC contains an invalid header. For instance, the header length may not be correct.

**Flow Drops:**
- **cxsc-request**—The CXSC requested to terminate the flow. The actions bit 0 is set.
- **reset-by-cxsc**—The CXSC requested to terminate and reset the flow. The actions bit 1 is set.
- **cxsc-fail-close**—The flow was terminated because the card is down and the configured policy was ‘fail-close.’

### Troubleshooting Problems with the Authentication Proxy

If you are having a problem using the authentication proxy feature, follow these steps to troubleshoot your configuration and connections.

**Note**

If you have a connection between hosts on two ASA interfaces, and the ASA CX service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA CX module, including traffic originating on the non-ASA CX interface (the feature is bidirectional). However, the ASA only performs the authentication proxy on the interface to which the service policy is applied, because this feature is ingress-only.

**Procedure**

**Step 1** Check your configurations.
- On the ASA, check the output of the **show asp table classify domain cxsc-auth-proxy** command and make sure there are rules installed and that they are correct.
- In PRSM, ensure the directory realm is created with the correct credentials and test the connection to make sure you can reach the authentication server; also ensure that a policy object or objects are configured for authentication.

**Step 2** Check the output of the **show service-policy cxsc** command to see if any packets were proxied.
Step 3  Perform a packet capture on the backplane (capture name interface asa_dataplane), and check to see if traffic is being redirected on the correct configured port. You can check the configured port using the show running-config cxsc command or the show asp table classify domain cxsc-auth-proxy command.

Example
Make sure port 2000 is used consistently:

1. Check the authentication proxy port:

   hostname# show running-config cxsc
   cxsc auth-proxy port 2000

2. Check the authentication proxy rules:

   hostname# show asp table classify domain cxsc-auth-proxy

   Input Table
   in id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
   hits=0, user_data=0x7ffed86ca220, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0
   dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
   input_ifc=inside, output_ifc=identity

3. In the packet captures, the redirect request should be going to destination port 2000.

History for the ASA CX Module

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5585-X with SSP-10 and -20 support for the ASA CX SSP-10 and -20</td>
<td>ASA 8.4(4.1) ASA CX 9.0(1)</td>
<td>The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same access to other employees. We introduced the following screens: Home &gt; ASA CX Status Wizards &gt; Startup Wizard &gt; ASA CX Basic Configuration Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA CX Inspection</td>
</tr>
</tbody>
</table>
### History for the ASA CX Module

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5512-X through ASA 5555-X support for the ASA CX SSP</td>
<td>ASA 9.1(1)</td>
<td>We introduced support for the ASA CX SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. We did not modify any screens.</td>
</tr>
<tr>
<td></td>
<td>ASA CX 9.1(1)</td>
<td></td>
</tr>
<tr>
<td>Monitor-only mode for demonstration purposes</td>
<td>ASA 9.1(2)</td>
<td>For demonstration purposes only, you can enable monitor-only mode for the service policy, which forwards a copy of traffic to the ASA CX module, while the original traffic remains unaffected.</td>
</tr>
<tr>
<td></td>
<td>ASA CX 9.1(2)</td>
<td>Another option for demonstration purposes is to configure a traffic-forwarding interface instead of a service policy in monitor-only mode. The traffic-forwarding interface sends all traffic directly to the ASA CX module, bypassing the ASA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following screen: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule &gt; Rule Actions &gt; ASA CX Inspection. The traffic-forwarding feature is supported by CLI only.</td>
</tr>
<tr>
<td>NAT 64 support for the ASA CX module</td>
<td>ASA 9.1(2)</td>
<td>You can now use NAT 64 in conjunction with the ASA CX module. We did not modify any screens.</td>
</tr>
<tr>
<td></td>
<td>ASA CX 9.1(2)</td>
<td></td>
</tr>
<tr>
<td>ASA 5585-X with SSP-40 and -60 support for the ASA CX SSP-40 and -60</td>
<td>ASA 9.1(3)</td>
<td>ASA CX SSP-40 and -60 modules can be used with the matching level ASA 5585-X with SSP-40 and -60. We did not modify any screens.</td>
</tr>
<tr>
<td></td>
<td>ASA CX 9.2(1)</td>
<td></td>
</tr>
<tr>
<td>Multiple context mode support for the ASA CX module</td>
<td>ASA 9.1(3)</td>
<td>You can now configure ASA CX service policies per context on the ASA.</td>
</tr>
<tr>
<td></td>
<td>ASA CX 9.2(1)</td>
<td>Note Although you can configure per context ASA service policies, the ASA CX module itself (configured in PRSM) is a single context mode device; the context-specific traffic coming from the ASA is checked against the common ASA CX policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We did not modify any screens.</td>
</tr>
</tbody>
</table>
Filtering packets captured on the ASA CX backplane

You can now filter packets captured on the ASA CX backplane using the `match` or `access-list` keyword with the `capture interface asa_dataplane` command.

Control traffic specific to the ASA CX module is not affected by the access-list or match filtering; the ASA captures all control traffic.

In multiple context mode, configure the packet capture per context. Note that all control traffic in multiple context mode goes only to the system execution space. Because control traffic cannot be filtered using an access-list or match, these options are not available in the system execution space.

We did not modify any ASDM screens.
ASA IPS Module

This chapter describes how to configure the ASA IPS module. The ASA IPS module might be a hardware module or a software module, depending on your ASA model. For a list of supported ASA IPS modules per ASA model, see the Cisco ASA Compatibility Matrix:


- Information About the ASA IPS Module, page 19-1
- Licensing Requirements for the ASA IPS module, page 19-4
- Guidelines and Limitations, page 19-5
- Default Settings, page 19-6
- Configuring the ASA IPS module, page 19-6
- Managing the ASA IPS module, page 19-17
- Monitoring the ASA IPS module, page 19-22
- Feature History for the ASA IPS module, page 19-23

Information About the ASA IPS Module

The ASA IPS module runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network.

- How the ASA IPS Module Works with the ASA, page 19-1
- Operating Modes, page 19-2
- Using Virtual Sensors, page 19-3
- Information About Management Access, page 19-4

How the ASA IPS Module Works with the ASA

The ASA IPS module runs a separate application from the ASA. The ASA IPS module might include an external management interface so you can connect to the ASA IPS module directly; if it does not have a management interface, you can connect to the ASA IPS module through the ASA interface. The ASA IPS SSP on the ASA 5585-X includes data interfaces; these interfaces provide additional port-density for the ASA. However, the overall throughput of the ASA is not increased.
Traffic goes through the firewall checks before being forwarded to the ASA IPS module. When you identify traffic for IPS inspection on the ASA, traffic flows through the ASA and the ASA IPS module as follows. **Note:** This example is for “inline mode.” See Operating Modes, page 19-2 for information about “promiscuous mode,” where the ASA only sends a copy of the traffic to the ASA IPS module.

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA IPS module.
5. The ASA IPS module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA IPS 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.

Figure 19-1 shows the traffic flow when running the ASA IPS module in inline mode. In this example, the ASA IPS module automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the ASA.

![ASA IPS module Traffic Flow in the ASA: Inline Mode](image)

**Operating Modes**

You can send traffic to the ASA IPS module using one of the following modes:

- **Inline mode**—This mode places the ASA IPS module directly in the traffic flow (see Figure 19-1). No traffic that you identified for IPS inspection can continue through the ASA without first passing through, and being inspected by, the ASA IPS module. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the ASA IPS module can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.

- **Promiscuous mode**—This mode sends a duplicate stream of traffic to the ASA IPS module. This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, in promiscuous mode the ASA IPS module can only block traffic by instructing the ASA to shun the traffic or by resetting a connection on the ASA. Also, while the ASA IPS module is analyzing the traffic, a small amount of traffic might pass through the ASA before the ASA IPS module can shun it. Figure 19-2
shows the ASA IPS module in promiscuous mode. In this example, the ASA IPS module sends a shun message to the ASA for traffic it identified as a threat.

**Figure 19-2  ASA IPS module Traffic Flow in the ASA: Promiscuous Mode**

Using Virtual Sensors

The ASA IPS module running IPS software Version 6.0 and later can run multiple virtual sensors, which means you can configure multiple security policies on the ASA IPS module. You can assign each ASA security context or single mode ASA to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

**Figure 19-3** shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

**Figure 19-3  Security Contexts and Virtual Sensors**

**Figure 19-4** shows a single mode ASA paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.
Information About Management Access

You can manage the IPS application using the following methods:

- Sessioning to the module from the ASA—If you have CLI access to the ASA, then you can session to the module and access the module CLI. See Sessioning to the Module from the ASA (May Be Required), page 19-10.

- Connecting to the IPS management interface using ASDM or SSH—After you launch ASDM from the ASA, your management station connects to the module management interface to configure the IPS application. For SSH, you can access the module CLI directly on the module management interface. (Telnet access requires additional configuration in the module application). The module management interface can also be used for sending syslog messages or allowing updates for the module application, such as signature database updates.

See the following information about the management interface:

- ASA 5585-X—The IPS management interface is a separate external Gigabit Ethernet interface.

- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X—These models run the ASA IPS module as a software module. The IPS management interface shares the Management 0/0 interface with the ASA. Separate MAC addresses and IP addresses are supported for the ASA and ASA IPS module. You must perform configuration of the IPS IP address within the IPS operating system (using the CLI or ASDM). However, physical characteristics (such as enabling the interface) are configured on the ASA. You can remove the ASA interface configuration (specifically the interface name) to dedicate this interface as an IPS-only interface. This interface is management-only.

Licensing Requirements for the ASA IPS module

The following table shows the licensing requirements for this feature:
This section includes the guidelines and limitations for this feature.

**Model Support**
- See the [Cisco ASA Compatibility Matrix](http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html) for information about which models support which modules.

**Additional Guidelines**
- ASDM 7.3(2) and later is not compatible with IPS 7.3(2) or earlier. To manage IPS, connect to its IP address directly in your browser.
- The total throughput for the ASA plus the IPS module is lower than ASA throughput alone.
- You cannot change the software type installed on the module; if you purchase an ASA IPS module, you cannot later install other software on it.
Default Settings

Table 19-1 lists the default settings for the ASA IPS module.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.1.1/24 (the default ASA management IP address)</td>
</tr>
<tr>
<td>Username</td>
<td>cisco</td>
</tr>
<tr>
<td>Password</td>
<td>cisco</td>
</tr>
</tbody>
</table>

Note

The default management IP address on the ASA is 192.168.1.1/24.

Configuring the ASA IPS module

This section describes how to configure the ASA IPS module.

- Task Flow for the ASA IPS Module, page 19-6
- Connecting the ASA IPS Management Interface, page 19-7
- Sessioning to the Module from the ASA (May Be Required), page 19-10
- Configuring Basic IPS Module Network Settings, page 19-11
- (ASA 5512-X through ASA 5555-X) Booting the Software Module, page 19-11
- Assigning Virtual Sensors to a Security Context, page 19-15
- Diverting Traffic to the ASA IPS module, page 19-16

Task Flow for the ASA IPS Module

Configuring the ASA IPS module is a process that includes configuration of the IPS security policy on the ASA IPS module and then configuration of the ASA to send traffic to the ASA IPS module. To configure the ASA IPS module, perform the following steps:

Step 1  Cable the ASA IPS management interface. See Connecting the ASA IPS Management Interface, page 19-7.

Step 2  Session to the module. Access the IPS CLI over the backplane. For ASDM users, you may need to session to the module to boot the IPS software if it is not running. See Sessioning to the Module from the ASA (May Be Required), page 19-10.

Step 3  (ASA 5512-X through ASA 5555-X; may be required) Install the software module. See (ASA 5512-X through ASA 5555-X) Booting the Software Module, page 19-11.

Step 5  On the module, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. See Configuring the Security Policy on the ASA IPS Module, page 19-13.

Step 6  (Optional) On the ASA in multiple context mode, specify which IPS virtual sensors are available for each context (if you configured virtual sensors). See Assigning Virtual Sensors to a Security Context, page 19-15.

Step 7  On the ASA, identify traffic to divert to the ASA IPS module. See Diverting Traffic to the ASA IPS module, page 19-16.

Connecting the ASA IPS Management Interface

In addition to providing management access to the IPS module, the IPS management interface needs access to an HTTP proxy server or a DNS server and the Internet so it can download global correlation, signature updates, and license requests. This section describes recommended network configurations. Your network may differ.

- ASA 5585-X (Hardware Module), page 19-7
- ASA 5512-X through ASA 5555-X (Software Module), page 19-8

ASA 5585-X (Hardware Module)

The IPS module includes a separate management interface from the ASA.

If you have an inside router

If you have an inside router, you can route between the management network, which can include both the ASA Management 0/0 and IPS Management 1/0 interfaces, and the ASA inside network. Be sure to also add a route on the ASA to reach the Management network through the inside router.
If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network, which would require an inside router to route between the networks. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. Because the IPS module is a separate device from the ASA, you can configure the IPS Management 1/0 address to be on the same network as the inside interface.

ASA 5512-X through ASA 5555-X (Software Module)

These models run the IPS module as a software module, and the IPS management interface shares the Management 0/0 interface with the ASA.
If you have an inside router

If you have an inside router, you can route between the Management 0/0 network, which includes both the ASA and IPS management IP addresses, and the inside network. Be sure to also add a route on the ASA to reach the Management network through the inside router.

Note
You must remove the ASA-configured name for Management 0/0; if it is configured on the ASA, then the IPS address must be on the same network as the ASA, and that excludes any networks already configured on other ASA interfaces. If the name is not configured, then the IPS address can be on any network, for example, the ASA inside network.

What to Do Next

Sessioning to the Module from the ASA (May Be Required)

To access the IPS module CLI from the ASA, you can session from the ASA. For software modules, 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.

You may need to access the CLI if you are using multiple context mode and you need to set basic network settings using the CLI, or for troubleshooting.

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet session. For a hardware module (for example, the ASA 5585-X): session 1</td>
<td>Accesses the module using Telnet. You are prompted for the username and password. The default username is cisco, and the default password is cisco. Note The first time you log in to the module, you are prompted to change the default password. Passwords must be at least eight characters long and cannot be a word in the dictionary.</td>
</tr>
<tr>
<td>For a software module (for example, the ASA 5545-X): session ips</td>
<td></td>
</tr>
<tr>
<td>Console session (software module only). session ips console</td>
<td>Accesses the module console. You are prompted for the username and password. The default username is cisco, and the default password is cisco. Note Do not use this 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 escape sequence to escape the IPS console and return to the ASA prompt. Therefore, if you try to exit the IPS 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 IPS 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 ips command instead.</td>
</tr>
<tr>
<td>Example: hostname# session 1</td>
<td>Opening command session with slot 1. Connected to slot 1. Escape character sequence is ‘CTRL-~X’. sensor login: cisco Password: cisco</td>
</tr>
<tr>
<td></td>
<td>Accesses the module console. You are prompted for the username and password. The default username is cisco, and the default password is cisco. Note Do not use this 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 escape sequence to escape the IPS console and return to the ASA prompt. Therefore, if you try to exit the IPS 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 IPS 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 ips command instead.</td>
</tr>
<tr>
<td>Example: hostname# session ips console</td>
<td>Establishing console session with slot 1 Opening console session with module ips. Connected to module ips. Escape character sequence is ‘CTRL-SHIFT-6 then x’. sensor login: cisco Password: cisco</td>
</tr>
</tbody>
</table>
(ASA 5512-X through ASA 5555-X) Booting the Software Module

Your ASA typically ships with IPS module software present on Disk0. If the module is not running, or if you are adding the IPS module to an existing ASA, you must boot the module software. If you are unsure if the module is running, you will not see the IPS Basic Configuration screen when you run the Startup Wizard (see Configuring Basic IPS Module Network Settings, page 19-11).

Detailed Steps

Step 1  Do one of the following:

- New ASA with IPS pre-installed—To view the IPS module software filename in flash memory, choose Tools > File Management.
  
  For example, look for a filename like IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip. Note the filename; you will need this filename later in the procedure.

- Existing ASA with new IPS installation—Download the IPS software from Cisco.com to your computer. If you have a Cisco.com login, you can obtain the software from the following website:
  

  Choose Tools > File Management, then choose File Transfer > Between Local PC and Flash to upload the new image to disk0. Note the filename; you will need this filename later in the procedure.

Step 2  Choose Tools > Command Line Interface.

Step 3  To set the IPS module software location in disk0, enter the following command and then click Send:

  sw-module module ips recover configure image disk0:file_path

  For example, using the filename in the example in Step 1, enter:

  sw-module module ips recover configure image disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip

Step 4  To install and load the IPS module software, enter the following command and then click Send:

  sw-module module ips recover boot

Step 5  To check the progress of the image transfer and module restart process, enter the following command and then click Send:

  show module ips details

  The Status field in the output indicates the operational status of the module. A module operating normally shows a status of “Up.” While the ASA transfers an application image to the module, the Status field in the output reads “Recover.” When the ASA completes the image transfer and restarts the module, the newly transferred image is running.

Configuring Basic IPS Module Network Settings

In single context mode, you can use the Startup Wizard in ASDM to configure basic IPS network configuration. These settings are saved to the IPS configuration, not the ASA configuration.
In multiple context mode, session to the module from the ASA and configure basic settings using the `setup` command.

**Note**  
(ASA 5512-X through ASA 5555-X) If you do not see the IPS Basic Configuration screen in your wizard, then the IPS module is not running. See (ASA 5512-X through ASA 5555-X) Booting the Software Module, page 19-11, and then repeat this procedure after you install the module.

### Detailed Steps—Single Mode

- **Step 1** Choose Wizards > Startup Wizard.
- **Step 2** Click Next to advance through the initial screens until you reach the IPS Basic Configuration screen.
- **Step 3** In the Network Settings area, configure the following:
  - IP Address—The management IP address. By default, the address is 192.168.1.2.
  - Subnet Mask—The subnet mask for the management IP address.
  - Gateway—The IP address of the upstream router. The IP address of the next hop router. See Connecting the ASA IPS Management Interface, page 19-7 to understand the requirements for your network. The default setting of the ASA management IP address will not work.
  - HTTP Proxy Server—(Optional) The HTTP proxy server address. You can use a proxy server to download global correlation updates and other information instead of downloading over the Internet.
  - HTTP Proxy Port—(Optional) The HTTP proxy server port.
  - DNS Primary—(Optional) The primary DNS server address. If you are using a DNS server, you must configure at least one DNS server and it must be reachable for global correlation updates to be successful.

  For global correlation to function, you must have either a DNS server or an HTTP proxy server configured at all times. DNS resolution is supported only for accessing the global correlation update server.

- **Step 4** In the Management Access List area, enter an IP address and subnet mask for any hosts that are allowed to access the IPS management interface, and click Add. You can add multiple IP addresses.
- **Step 5** In the Cisco Account Password area, set the password for the username `cisco` and confirm it. The username `cisco` and this password are used for Telnet sessions from hosts specified by the management ACL and when accessing the IPS module from ASDM (Configuration > IPS). By default, the password is `cisco`.
- **Step 6** In the Network Participation area, which you use to have the IPS module participate in SensorBase data sharing, click Full, Partial, or Off.
Detailed Steps—Multiple Mode Using the CLI

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Session to the IPS module according to Sessioning to the Module from the ASA (May Be Required), page 19-10.</td>
</tr>
<tr>
<td>Step 2 setup</td>
<td>Runs the setup utility for initial configuration of the ASA IPS module. You are prompted for basic settings. For the default gateway, specify the IP address of the upstream router. See Connecting the ASA IPS Management Interface, page 19-7 to understand the requirements for your network. The default setting of the ASA management IP address will not work.</td>
</tr>
</tbody>
</table>

Configuring the Security Policy on the ASA IPS Module

This section describes how to configure the ASA IPS module application.

Detailed Steps

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Connect to ASDM using the ASA management IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To access the IPS Device Manager (IDM) from ASDM, click Configuration &gt; IPS.</td>
</tr>
</tbody>
</table>

Step 3
Enter the IP address, username and password that you set in the Configuring Basic IPS Module Network Settings, page 19-11, as well as the port. The default IP address and port is 192.168.1.2:443. The default username and password is *cisco* and *cisco*.

If the password to access IDM is lost, you can reset the password using ASDM. See Resetting the Password, page 19-21, for more information.

Step 4
To save the login information on your local PC, check the Save IPS login information on local host check box.

Step 5
Click Continue. The Startup Wizard pane appears.
Click **Launch Startup Wizard**. Complete the screens as prompted. For more information, see the IDM online help.

If you configure virtual sensors, you identify one of the sensors as the default. If the ASA series does not specify a virtual sensor name in its configuration, the default sensor is used.

**What to Do Next**

- For the ASA in multiple context mode, see Assigning Virtual Sensors to a Security Context, page 19-15.
- For the ASA in single context mode, see Diverting Traffic to the ASA IPS module, page 19-16.
Assigning Virtual Sensors to a Security Context

If the ASA is in multiple context mode, then you can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the ASA IPS module, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the ASA IPS module is used. You can assign the same sensor to multiple contexts.

**Note**
You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

**Prerequisites**
For more information about configuring contexts, see the general operations configuration guide.

**Detailed Steps**

**Step 1** In the ASDM Device List pane, double-click **System** under the active device IP address.

**Step 2** On the Context Management > Security Contexts pane, choose a context that you want to configure, and click **Edit**.

The Edit Context dialog box appears. For more information about configuring contexts, see the general operations configuration guide.

**Step 3** In the IPS Sensor Allocation area, click **Add**.

The IPS Sensor Selection dialog box appears.

**Step 4** From the Sensor Name drop-down list, choose a sensor name from those configured on the ASA IPS module.

**Step 5** (Optional) To assign a mapped name to the sensor, enter a value in the Mapped Sensor Name field.

This sensor name can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” sensors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.

**Step 6** Click **OK** to return to the Edit Context dialog box.

**Step 7** (Optional) To set one sensor as the default sensor for this context, from the Default Sensor drop-down list, choose a sensor name.

If you do not specify a sensor name when you configure IPS within the context configuration, the context uses this default sensor. You can only configure one default sensor per context. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the ASA IPS module.

**Step 8** Repeat this procedure for each security context.
Step 9 Change to each context to configure the IPS security policy as described in Diverting Traffic to the ASA IPS module, page 19-16.

What to Do Next

Change to each context to configure the IPS security policy as described in Diverting Traffic to the ASA IPS module, page 19-16.

Diverting Traffic to the ASA IPS module

This section identifies traffic to divert from the ASA to the ASA IPS module.

Prerequisites

In multiple context mode, perform these steps in each context execution space. To change to a context, in the Configuration > Device List pane, double-click the context name under the active device IP address.

Detailed Steps

Step 1 Choose Configuration > Firewall > Service Policy Rules.


Step 3 Complete the Service Policy dialog box as desired. See the ASDM online help for more information about these screens.

Step 4 Click Next. The Add Service Policy Rule Wizard - Traffic Classification Criteria dialog box appears.

Step 5 Complete the Traffic Classification Criteria dialog box as desired. See the ASDM online help for more information about these screens.
Step 6  Click **Next** to show the Add Service Policy Rule Wizard - Rule Actions dialog box.

Step 7  Click the **Intrusion Prevention** tab.

![Add Service Policy Rule Wizard - Rule Actions](image)

Step 8  Check the **Enable IPS for this traffic flow** check box.

Step 9  In the Mode area, click **Inline Mode** or **Promiscuous Mode**. See Operating Modes, page 19-2 for more information.

Step 10  In the If IPS Card Fails area, click **Permit traffic** or **Close traffic**. The Close traffic option sets the ASA to block all traffic if the ASA IPS module is unavailable. The Permit traffic option sets the ASA to allow all traffic through, uninspected, if the ASA IPS module is unavailable. For information about the IPS Sensor Selection area, see the ASDM online help.

Step 11  (ASA 5512-X and higher) From the IPS Sensor to use drop-down list, choose a virtual sensor name. If you use virtual sensors, you can specify a sensor name using this option. If you use multiple context mode on the ASA, you can only specify sensors that you assigned to the context (see Assigning Virtual Sensors to a Security Context, page 19-15). If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the ASA IPS module.

Step 12  Click **OK** and then **Apply**.

Step 13  Repeat this procedure to configure additional traffic flows as desired.

---

**Managing the ASA IPS module**

This section includes procedures that help you recover or troubleshoot the module.

- Installing and Booting an Image on the Module, page 19-18
- Shutting Down the Module, page 19-20
- Uninstalling a Software Module Image, page 19-20
- Resetting the Password, page 19-21
•  Reloading or Resetting the Module, page 19-22

Installing and Booting an Image on the Module

If the module suffers a failure, and the module application image cannot run, you can reinstall a new image on the module from a TFTP server (for a hardware module), or from the local disk (software module).

Note
Do not use the upgrade command within the module software to install the image.

Prerequisites

•  Hardware module—Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

  Note
This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

•  Software module—Copy the image to the ASA internal flash (disk0) before completing this procedure.

  Note
Before you download the IPS software to disk0, make sure at least 50% of the flash memory is free. When you install IPS, IPS reserves 50% of the internal flash memory for its file system.
### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies the location of the new image.</td>
</tr>
<tr>
<td>For a hardware module (for example, the ASA 5585-X):</td>
<td></td>
</tr>
<tr>
<td><code>hw-module module 1 recover configure</code></td>
<td></td>
</tr>
<tr>
<td>For a software module (for example, the ASA 5545-X):</td>
<td>Specifies the location of the new image.</td>
</tr>
<tr>
<td><code>sw-module module ips recover configure image disk0:file_path</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>hostname# hw-module module 1 recover configure</code></td>
<td></td>
</tr>
<tr>
<td><code>Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg</code></td>
<td></td>
</tr>
<tr>
<td><code>Port IP Address [127.0.0.2]: 10.1.2.10</code></td>
<td></td>
</tr>
<tr>
<td><code>Port Mask [255.255.255.254]: 255.255.255.0</code></td>
<td></td>
</tr>
<tr>
<td><code>Gateway IP Address [1.1.2.10]: 10.1.2.254</code></td>
<td></td>
</tr>
<tr>
<td><code>VLAN ID [0]: 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Installs and boots the IPS module software.</td>
</tr>
<tr>
<td>For a hardware module:</td>
<td></td>
</tr>
<tr>
<td><code>hw-module module 1 recover boot</code></td>
<td></td>
</tr>
<tr>
<td>For a software module:</td>
<td></td>
</tr>
<tr>
<td><code>sw-module module ips recover boot</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>hostname# hw-module module 1 recover boot</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Checks the progress of the image transfer and module restart process. The Status field in the output indicates the operational status of the module. A module operating normally shows a status of “Up.” While the ASA transfers an application image to the module, the Status field in the output reads “Recover.” When the ASA completes the image transfer and restarts the module, the newly transferred image is running.</td>
</tr>
<tr>
<td>For a hardware module:</td>
<td></td>
</tr>
<tr>
<td><code>show module 1 details</code></td>
<td></td>
</tr>
<tr>
<td>For a software module:</td>
<td></td>
</tr>
<tr>
<td><code>show module ips details</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>hostname# show module 1 details</code></td>
<td></td>
</tr>
</tbody>
</table>
Shutting Down the Module

Shutting down the module software prepares the module to be safely powered off without losing configuration data. **Note:** If you reload the ASA, the module is not automatically shut down, so we recommend shutting down the module before reloading the ASA. To gracefully shut down the module, perform the following steps at the ASA CLI.

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a hardware module (for example, the ASA 5585-X):</td>
<td>Shuts down the module.</td>
</tr>
<tr>
<td>hw-module module 1 shutdown</td>
<td></td>
</tr>
<tr>
<td>For a software module (for example, the ASA 5545-X):</td>
<td></td>
</tr>
<tr>
<td>sw-module module ips shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

hostname# hw-module module 1 shutdown

**Uninstalling a Software Module Image**

To uninstall a software module image and associated configuration, perform the following steps.

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Permanently uninstalls the software module image and associated configuration.</td>
</tr>
<tr>
<td>sw-module module ips uninstall</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>hostname# sw-module module ips uninstall</td>
<td>Module ips will be uninstalled. This will completely remove the disk image associated with the sw-module including any configuration that existed within it.</td>
</tr>
<tr>
<td>Uninstall module &lt;id&gt;? [confirm]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Reloads the ASA. You must reload the ASA before you can install a new module type.</td>
</tr>
<tr>
<td>reload</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>hostname# reload</td>
<td></td>
</tr>
</tbody>
</table>
Resetting the Password

You can reset the module password to the default. For the user cisco, the default password is cisco. After resetting the password, you should change it to a unique value using the module application.

Resetting the module password causes the module to reboot. Services are not available while the module is rebooting.

If you cannot connect to ASDM with the new password, restart ASDM and try to log in again. If you defined a new password and still have an existing password in ASDM that is different from the new password, clear the password cache by choosing File > Clear ASDM Password Cache, then restart ASDM and try to log in again.

To reset the module password to the default of cisco, perform the following steps.

Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the ASDM menu bar, choose Tools &gt; module Password Reset. The Password Reset confirmation dialog box appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click OK to reset the password to the default. A dialog box displays the success or failure of the password reset.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Close to close the dialog box.</td>
</tr>
</tbody>
</table>
Reloading or Resetting the Module

To reload or reset the module, enter one of the following commands at the ASA CLI.

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a hardware module (for example, the ASA 5585-X):</td>
<td>Reloads the module software.</td>
</tr>
<tr>
<td>hw-module module 1 reload</td>
<td></td>
</tr>
<tr>
<td>For a software module (for example, the ASA 5545-X):</td>
<td></td>
</tr>
<tr>
<td>sw-module module ips reload</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>hostname# hw-module module 1 reload</td>
<td></td>
</tr>
<tr>
<td>For a hardware module:</td>
<td>Performs a reset, and then reloads the module.</td>
</tr>
<tr>
<td>hw-module module 1 reset</td>
<td></td>
</tr>
<tr>
<td>For a software module:</td>
<td></td>
</tr>
<tr>
<td>sw-module module ips reset</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>hostname# hw-module module 1 reset</td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring the ASA IPS module**

See the Intrusion Prevention Tab in the general operations configuration guide.
Feature History for the ASA IPS module

Table 19-2 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 19-2 Feature History for the ASA IPS module

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIP SSM</td>
<td>7.0(1)</td>
<td>We introduced support for the AIP SSM for the ASA 5510, 5520, and 5540. The following screen was introduced: Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Intrusion Prevention.</td>
</tr>
<tr>
<td>Virtual sensors (ASA 5510 and higher)</td>
<td>8.0(2)</td>
<td>Virtual sensor support was introduced. Virtual sensors let you configure multiple security policies on the ASA IPS module. The following screen was modified: Context Management &gt; Security Contexts &gt; Edit Context.</td>
</tr>
<tr>
<td>AIP SSC for the ASA 5505</td>
<td>8.2(1)</td>
<td>We introduced support for the AIP SSC for the ASA 5505. The following screen was introduced: Configuration &gt; Device Setup &gt; SSC Setup.</td>
</tr>
<tr>
<td>Support for the ASA IPS SSP-10, -20, -40, and -60 for the ASA 5585-X</td>
<td>8.2(5)/8.4(2)</td>
<td>We introduced support for the ASA IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the ASA IPS SSP with a matching-level SSP; for example, SSP-10 and ASA IPS SSP-10. Note The ASA 5585-X is not supported in Version 8.3.</td>
</tr>
<tr>
<td>Support for Dual SSPs for SSP-40 and SSP-60</td>
<td>8.4(2)</td>
<td>For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. Note When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled. We did not modify any screens.</td>
</tr>
<tr>
<td>Support for the ASA IPS SSP for the ASA 5512-X through ASA 5555-X</td>
<td>8.6(1)</td>
<td>We introduced support for the ASA IPS SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. We did not modify any screens.</td>
</tr>
</tbody>
</table>