Managing Firewall Inspection Rules

Inspection rules configure protocol inspection on a device. Inspection opens temporary holes in your access rules to allow return traffic for connections initiated within your trusted network. When traffic is inspected, the device also implements additional controls to eliminate mal-formed packets based on the inspected protocols.

Note From version 4.17, though Cisco Security Manager continues to support PIX, FWSM, and IPS features/functionality, it does not support any enhancements.

The device commands generated for inspection rules vary based on device type. For devices running ASA, PIX 7.0+, and FWSM 3.x+, access-list, policy-map, and class-map commands are used. For older FWSM and PIX 6.3 devices, fixup commands are used. For IOS devices, ip-inspect commands are used.

The following topics will help you work with inspection rules:

The following topics can help you with general rule table usage:

Understanding Inspection Rules

Inspection rules configure Context-Based Access Control (CBAC) inspection commands. CBAC inspects traffic that travels through the device to discover and manage state information for TCP and UDP sessions. The device uses this state information to create temporary openings to allow return traffic and additional data connections for permissible sessions.

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when inspected traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered inspection when exiting through the firewall.

Inspection rules are applied after your access rules, so any traffic that you deny in the access rule is not inspected. The traffic must be allowed by the access rules at both the input and output interfaces to be inspected. Whereas access rules allow you to control connections at layer 3 (network, IP) or 4 (transport, TCP or UDP protocol), you can use inspection rules to control traffic using application-layer protocol session information.

For all protocols, when you inspect the protocol, the device provides the following functions:

- Automatically opens a return path for the traffic (reversing the source and destination addresses), so that you do not need to create an access rule to allow the return traffic. Each connection is considered a session, and the device maintains session state information and allows return traffic only for valid sessions. Protocols that use TCP contain explicit session information, whereas for UDP applications, the device models the equivalent of a session based on the source and destination addresses and the closeness in time of a sequence of UDP packets.

  These temporary access lists are created dynamically and are removed at the end of a session.
- Tracks sequence numbers in all TCP packets and drops those packets with sequence numbers that are not within expected ranges.
- Uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. When a session is dropped, or reset, the device informs both the source and destination of the session to reset the connection, freeing up resources and helping to mitigate potential Denial of Service (DoS) attacks.

The following topics provide more information about inspection:

- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Inspection Rules, page 17-5
- Configuring Settings for Inspection Rules for IOS Devices, page 17-111

Choosing the Interfaces for Inspection Rules

Configure inspection on devices that protect internal networks. Use it with TCP, UDP, or more specific protocols. Inspect these applications if you want the application's traffic to be permitted through the device only when the traffic session is initiated from a particular side of the device (usually from the protected internal network).

Tip For IOS devices, you need to configure inspection explicitly, and you can identify the direction of traffic to be inspected. For ASA, PIX, and FWSM devices, you cannot identify the direction, and you need to configure inspection only if you do not want the inspection defaults. In the remaining discussion, statements concerning direction apply only to IOS devices. For ASA, PIX, and FWSM, simply configure inspection on the identified interface.

In many cases, you will configure inspection in one direction only at a single interface, which causes traffic to be permitted back into the internal network only if the traffic is part of a permissible (valid, existing) session. This is a typical configuration for protecting your internal networks from traffic that originates on the Internet.

You can also configure inspection in two directions at one or more interfaces. Configure inspection in two directions when the networks on both sides of the firewall should be protected, such as with extranet or intranet configurations, and to protect against DoS attacks. For example, if the device is situated between two partner companies' networks, you might want to restrict traffic in one direction for certain applications, and restrict traffic in the opposite direction for other applications. If you are protecting a web server in the DMZ zone, you might want to configure deep inspection on HTTP traffic to identify and reset connections that have undesirable characteristics.

You might want to configure your inspection rules on the outbound interfaces of your network, those that connect to the Internet or another uncontrolled network, while allowing unfiltered connections within the trusted network. Thus, your devices use resources for inspection only on sessions that travel over unsecured and therefore potentially dangerous networks.

Related Topics

- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Inspection Rules, page 17-5

Selecting Which Protocols To Inspect

You can generically inspect TCP and UDP, which covers all applications that use these protocols. However, you can also inspect more specific protocols. In some cases, inspecting a specific protocol provides better service than generic TCP/UDP inspection. TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number than the previous exiting packet.

For example:

- Some protocols allow you to configure deep inspection. Deep inspection allows you to configure more specific rules for a traffic stream. For example, you can drop HTTP connections where the content type of the request and response do not match. For information on deep inspection and your configuration options, see Configuring Protocols and Maps for Inspection, page 17-22.
- Protocols that negotiate return channels, such as FTP, should be specifically inspected. If you use simple generic TCP inspection of FTP traffic, the negotiated channels are not opened, and the connection will fail. If you want to allow FTP, ensure that you create a specific inspection rule for it.

Multimedia protocols also negotiate return channels and should be specifically inspected. These include H.323, RTSP (Real Time Streaming Protocol), and other application-specific protocols. Some applications also use a generic TCP channel, so you might also need to configure generic TCP inspection. Any generic TCP inspection rule should appear below a more specific inspection rule in the table (that is, any rule that specifies TCP or UDP should appear at the end of the inspection rule table).

Related Topics

- Choosing the Interfaces for Inspection Rules, page 17-2
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5

Understanding Access Rule Requirements for Inspection Rules

Access rules are applied before inspection rules. Therefore, you must ensure that your access rules do not prohibit traffic that you want inspected. Use the following guidelines:

- Permit inspected traffic to leave the network through the firewall.

  All access rules that evaluate traffic leaving the protected network should permit traffic that will be inspected. For example, if Telnet will be inspected, then Telnet traffic should be permitted on all access rules that apply to traffic leaving the network.

- Deny inspected return traffic entering the network through the firewall.

  For temporary openings to be created in an access list, the access list should deny inspected return traffic because the inspection engine will open up temporary holes in the access lists for this traffic. (You want traffic to be normally blocked when it enters your network.)

- Permit or deny traffic that cannot be inspected, or that you do not want to inspect, as required by your network.

  For example, if you do not want to inspect ICMP traffic, but you want to allow some ICMP traffic, configure your access rules to allow the traffic in both directions. Consider permitting at least these ICMP message types: echo reply (for ping commands), time-exceeded (for trace route), packet-too-big (for path MTU discovery), traceroute (for trace route), and unreachable (to notify that a host cannot be found).

- Add an access rule entry denying any network traffic from a source address matching an address on the protected network.

  This is known as anti-spoofing protection because it prevents traffic from an unprotected network from assuming the identity of a device on the protected network.

- Add an entry denying broadcast messages with a source address of 255.255.255.255.

  This entry helps to prevent broadcast attacks.

Related Topics

- Understanding Access Rules, page 16-1
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Configuring Inspection Rules, page 17-5

Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX, FWSM, and IPS features/functionality, it does not support any enhancements.

Inspecting packets at the application layer, and maintaining TCP and UDP session information, provides a device with the ability to detect and prevent certain types of network attacks such as SYN-flooding. A SYN-flood attack occurs when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests. Network attacks that deny access to a network device are called denial-of-service (DoS) attacks.

Inspection helps to protect against DoS attacks in other ways. Inspection looks at packet sequence numbers in TCP connections to see if they are within expected ranges and drops any suspicious packets. You can also configure inspection to drop half-open connections, which require firewall processing and memory resources to maintain. Additionally, inspection can detect unusually high rates of new connections and issue alert messages.

For IOS devices, you can configure several inspection setting parameters to fine-tune your defenses against SYN flooding and half-open connections. Configure the **Firewall > Settings > Inspection** policy. For details about each setting, see Configuring Settings for Inspection Rules for IOS Devices, page 17-111.

Inspection can also help by protecting against certain DoS attacks involving fragmented IP packets. Even though the firewall prevents an attacker from making actual connections to a given host, the attacker can disrupt services provided by that host. This is done by sending many non-initial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets. To fine-tune fragment inspection, configure an inspection rule for the **fragment** protocol and configure the maximum number of fragments you want to allow and a timeout value.

Related Topics

- Understanding Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Inspection Rules, page 17-5

Configuring Inspection Rules

Inspection rules policies identify the traffic that will be inspected through an interface. Inspection tracks permitted sessions and opens temporary holes in your access rules to allow return traffic.

Inspection rules are processed after access rules, so any traffic dropped by an access rule is not inspected. You can also use deny rules to selectively exclude certain types of traffic from inspection. For example, you might create a deny inspection rule to prevent a specific class of DNS traffic from being inspected, while all other DNS traffic is inspected. The basic procedure is:

- Add a new deny rule before the default inspection rule for the specific protocol. For the Match Traffic By option, select Source and Destination Address and Port. Next, define the specific type of traffic by providing Source and Destination Network IP addresses, and selecting the desired Service type (for example, DNS-TCP). Finally, in the third screen of the inspection-rule wizard, select the appropriate protocol (for example, DNS).
- Now edit the default inspection rule (below your new deny rule in the table). Again select Source and Destination Address and Port for the Match Traffic By option. Be sure this is a Permit rule, provide an all-addresses option as the source and destination addresses, and enter IP as the Service type. In the third screen, keep the selected protocol; configure or remove the related map, as necessary.

See Inspection Rules Page, page 17-8 and Add or Edit Inspect/Application FW Rule Wizard, page 17-11 for additional information about this process.

See the following topics for more information about things you should consider when creating inspection rules:

- Understanding Inspection Rules, page 17-2
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Protocols and Maps for Inspection, page 17-22
- Understanding Map Objects, page 6-78

Before You Begin

You might have a set of inspection rules that you want to apply to all devices. To do this, you can create a shared rule and inherit its rules to each device's inspection rules policy. For more information, see Creating a New Shared Policy, page 5-54 and Inheriting or Uninheriting Rules, page 5-47.

Step 1 Do one of the following to open the Inspection Rules Page, page 17-8:

- (Device view) Select **Firewall > Inspection Rules** from the Policy selector.
- (Policy view) Select **Firewall > Inspection Rules** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the row after which you want to create the rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add or Edit Inspect/Application FW Rule Wizard, page 17-11.

Tip If you do not select a row, the new rule is added at the end of the local scope. You can also select an existing row and edit either the entire row or specific cells. For more information, see Editing Rules, page 12-10.

Step 3 Select whether to apply the rule to all interfaces on the device or to only the interfaces you specify.

If you elect to specify interfaces, enter the interface name or interface role, or click **Select** to select it from a list. For IOS devices, you also can select whether the rule applies in the Out direction (traffic leaving the interface). Use the In direction for all other device types.

Step 4 Select the criteria you want to use for matching traffic. This determines what gets inspected based on this rule.

- **Default Protocol Ports**—Select this option if the protocol you are inspecting uses the default ports on your network.

  If you want to constrain the inspection based on the source or destination address, also select **Limit inspection between source and destination IP addresses** (available only for ASA, PIX 7.x+, and FWSM 3.x+ devices). When you click **Next**, you are prompted for the source and destination addresses. You can specify **any** for source or destination if you are interested only in configuring the other value.

- **Custom Destination Ports**—Select this option if you want to associate additional non-default TCP or UDP ports with a given protocol, for example, treating TCP traffic on destination port 8080 as HTTP traffic. When you click **Next**, you are prompted for the port or port range.

- **Destination Address and Port (IOS devices only)**—Select this option if you want to associate additional non-default TCP or UDP ports with a given protocol only when the traffic is going to certain destinations, for example, if you want to treat TCP traffic on destination port 8080 as HTTP only when the traffic is going to server 192.168.1.10. When you click **Next**, you are prompted for the destination address and the port information.

- **Source and Destination Address and Port (PIX 7.x+, ASA, FWSM 3.x+)**—Select this option for the same reason you would select Destination Address and Port for IOS devices, although you have the additional option of identifying the source of the traffic. When you click **Next**, you are prompted for the source and destination addresses and the service port information.

Note For FWSM 2.x and PIX 6.3(x), you can select either Default Inspection Traffic or Custom Destination Ports only.

Step 5 Click **Next**. If you selected anything other than Default Protocol Ports, fill in the required addressing and port information explained above and click **Next**. See Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13.

Step 6 On the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select the protocol you want to inspect from the list. Ensure that the Device Type field indicates that inspection is supported for that protocol on the devices to which you are assigning the rule. (If you assign a rule to an unsupported device type, the rule is ignored but you will get a validation warning).

If the protocol you select allows additional configuration, the **Configure** button becomes active. Click it to view and select your options. For more information, see Configuring Protocols and Maps for Inspection, page 17-22.

For IOS devices only:

- If you selected **Custom Destination Ports** or **Destination Address and Port** as the traffic match, you can select **custom protocol** as the protocol name and click **Configure** to assign a name to the configuration.
- You can configure additional alert, audit, and timeout settings that override those set in the inspection settings policy. You can also specify whether to inspect router generated traffic for a limited number of protocols. For more information about inspection settings, see Configuring Settings for Inspection Rules for IOS Devices, page 17-111.

Step 7 Click **Finish** to save the rule.

Step 8 If you did not select the right row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.

Note From ASA 9.9.1, for cluster mode devices which are enabled with Security Gateway feature, the following list of centralized inspections are disabled:

- DCERPC
- NetBIOS
- PPTP
- RADIUS
- RSH
- SUNRPC
- TFTP
- XDMCP

During preview config, if inspection rules are configured for the unsupported devices, a validation error is displayed.

Note When there is rollback of device, the default dns policy-map configuration is automatically added to the device. Thus, after Cisco Security Manager processes the device rollback, on re-discovery of the device, the default dns-policy-map configuration is discovered in Cisco Security Manager.

Inspection Rules Page

Use the Inspection Rules page to configure inspection rules for device interfaces. Inspection examines traffic that travels through the device to discover and manage state information for TCP and UDP sessions. The device uses this state information to create temporary openings to allow return traffic and additional data connections for permissible sessions.

Note With the release of Security Manager 4.4 and versions 9.0 and higher of the ASA, the separate policies and objects for configuring IPv4 and IPv6 inspection rules were "unified," meaning one set of inspection rules in which you can use either IPv4 or IPv6 addresses, or a mixture of both. (See Policy Object Changes in Security Manager 4.4, page 1-10 for additional information.) In Policy view, IPv4 and unified versions of the inspection policy type are provided. In addition, a utility that you can use to convert existing IPv4 policies is provided (see Converting IPv4 Rules to Unified Rules, page 12-28). The following descriptions apply to all versions of the inspection rule table, except where noted.

If you assign an IPv4 inspection-rule shared policy to a 9.0+ device, you will no longer be able to assign unified versions of those policies to that device. Likewise, if you assign a unified inspection-rule shared policy to a 9.0+ device, you will no longer be able to assign IPv4 versions of those shared policies to that device--the device will not be included in the list of available devices on the Assignments tab for the shared policy.

Inspection rules are processed after your access rules. Thus, any traffic denied by an access rule is never inspected.

Read the following topics before you configure inspection rules:

- Understanding Inspection Rules, page 17-2
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5

Tip Disabled rules are shown with hash marks covering the table row. When you deploy the configuration, disabled rules are removed from the device. For more information, see Enabling and Disabling Rules, page 12-20.

Navigation Path

To access the Inspection Rules page, do one of the following:

- (Device view) Select a device, then select **Firewall > Inspection Rules** from the Policy selector.
- (Policy view) Select **Firewall > Inspection Rules** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Policies > Inspection Rules**.

Related Topics

- Adding and Removing Rules, page 12-9
- Editing Rules, page 12-10
- Enabling and Disabling Rules, page 12-20
- Moving Rules and the Importance of Rule Order, page 12-19
- Using Sections to Organize Rules Tables, page 12-20
- Using Rules Tables, page 12-8
- Filtering Tables, page 1-48

Field Reference

Table 17-1 Inspection Rules Page

Element	Description
Expand all rows/Collapse all rows	Use these buttons to expand or collapse all sections in the rules table. **Note** The buttons are located in the upper-right corner of the Filter area above the inspection rules table.
Conflict Indicator icons	Identifies conflicts and provides a quick visual representation of the type of conflict. For more details, including types of conflicts and the actions you can take from this column, see Understanding the Automatic Conflict Detection User Interface, page 16-30.
No.	The ordered rule number.

Table 17-1 Inspection Rules Page (continued)

Element	Description
Permit	Whether a rule identifies traffic that should be inspected based on the conditions set: • Permit—Identifies traffic that will be inspected. Shown as a green check mark. • Deny—Exempts the traffic from inspection. Your access rules will determine if the traffic is allowed or blocked. Shown as a red circle with slash.
Sources	The sources of traffic for this rule; can be networks, security groups (ASA 9.0+ only), and users. Multiple entries are displayed on separate lines within the table cell.
Destinations	The destinations for this rule; can be networks and security groups (ASA 9.0+ only). Multiple entries are displayed on separate lines within the table cell.
Traffic Match	The type of matching used in the rule: • **default-inspection**—The rule inspects traffic based on the default port. • TCP,UDP/port number—The rule inspects traffic based on a custom port number. • Service—The rule inspects traffic based on a service specification or service object. Multiple entries are displayed as separate subfields within the table cell. See Understanding and Specifying Services and Service and Port List Objects, page 6-100.
Interface	The interfaces or interface roles to which the rule is assigned. **Global** indicates that the rule is assigned to all interfaces. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. Multiple entries are displayed as separate subfields within the table cell. See Understanding Interface Role Objects, page 6-73.
Dir.	The direction of the traffic to which this rule applies: • In—Packets entering the interface. • Out—Packets exiting the interface.
Inspected Protocol	The protocol to be inspected and possibly some configuration settings for the protocol. You can right-click this cell and choose Edit Inspected Protocol to edit this; see Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17 for more information.
Time Range	The time range policy object assigned to the rule. This object defines the time window within which inspection occurs.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	The description of the rule, if any.

Table 17-1 Inspection Rules Page (continued)

Element	Description
Last Ticket(s)	Shows the ticket(s) associated with last modification to the rule. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page, page 11-72).
Page elements below the rules table	
Query	Click this button to run a policy query, which can help you evaluate your rules and identify ineffective rules. See Generating Policy Query Reports, page 12-28
Find and Replace button (binoculars icon)	Click this button to search for various types of items within the table and to optionally replace them. See Finding and Replacing Items in Rules Tables, page 12-16.
Up Row and Down Row buttons (arrow icons)	Click these buttons to move the selected rules up or down within a scope or section. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.
Add Row button	Click this button to add a rule to the table after the selected row using the Add or Edit Inspect/Application FW Rule Wizard, page 17-11. If you do not select a row, the rule is added at the end of the local scope. For more information about adding rules, see Adding and Removing Rules, page 12-9.
Edit Row button	Click this button to edit the selected rule. You can also edit individual cells. For more information, see Editing Rules, page 12-10.
Delete Row button	Click this button to delete the selected rule.

Add or Edit Inspect/Application FW Rule Wizard

Use the Add or Edit Inspect/Application FW Rule wizard to add and edit inspection rules. The wizard steps you through the process of configuring an inspection rule based on your selection in the **Match Traffic By** group on this page.

Read the following topics before you configure inspection rules:

- Understanding Inspection Rules, page 17-2
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5

Navigation Path

From the Inspection Rules Page, page 17-8, click the **Add Row** button or select a row and click the **Edit Row** button.

Related Topics

- Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13
- Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17
- Understanding Interface Role Objects, page 6-73
- Editing Rules, page 12-10

Field Reference

Table 17-2 Add and Edit Inspect/Application FW Rule Wizard Step 1: Traffic Match Method

Element	Description
Enable Rule	Whether to enable the rule, which means the rule becomes active when you deploy the configuration to the device. Disabled rules are shown overlain with hash marks in the rule table. For more information, see Enabling and Disabling Rules, page 12-20.
Apply the Rule to	The interface to which the rule applies: • All Interfaces—Apply the rule to all interfaces. The rule becomes a global rule on ASA, PIX, and FWSM devices. For IOS devices, the rule is configured for each interface in the In direction. • Interface (PIX 7.x+, ASA, FWSM 3.x+, IOS)—Apply the rule only to those interfaces identified in the Interfaces field. Enter the name of the interface or the interface role, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list. For IOS devices only, you can select the direction of the traffic to which this rule applies, either traffic entering an interface (**In**) or exiting it (**Out**). For other devices, leave **In** as the direction.
Match Traffic By How you want to identify the traffic to inspect. If you select something other than Default Protocol Ports (by itself), you are prompted for the other port or address information when you click **Next**.	
Default Protocol Ports Limit inspection between source and destination IP addresses (PIX 7.x+, ASA, FWSM 3.x+)	Inspect traffic based on the default ports assigned to a protocol. You will select a protocol on the next page (Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17). You can also select **Limit inspection between source and destination IP addresses** to configure the inspection to occur only between a specified source and destination. Do not select this option if you want to inspect a protocol without applying any constraints to the inspected traffic. If you also select this option, the next page of the wizard is described in Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13.

Table 17-2 Add and Edit Inspect/Application FW Rule Wizard Step 1: Traffic Match Method

Element	Description
Custom Destination Ports	Inspect traffic based on specified non-default TCP or UDP destination ports. Select this option if you want to associate additional TCP or UDP traffic with a given protocol, for example, treating TCP traffic on destination port 8080 as HTTP traffic. You will specify the protocol and port(s) on the next page of the wizard; see Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13.
Destination Address and Port (IOS devices only)	Inspect traffic on IOS devices based on destination IP address and port. Select this option if you want to associate additional non-default TCP or UDP ports with a given protocol only when the traffic is going to certain destinations, for example, if you want to treat TCP traffic on destination port 8080 as HTTP only when the traffic is going to server 192.168.1.10.
Source and Destination Address and Port (PIX 7.x, ASA, FWSM 3.x)	Inspect traffic on PIX 7.x+, ASA, and FWSM 3.x+ devices based on source and destination IP addresses and services. Select this option for the same reason you would select Destination Address and Port for IOS devices, although you have the additional option of identifying the source of the traffic. You will specify the action, sources, destinations, and Services on the next page of the wizard; see Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	An optional description of the rule (up to 1024 characters).

Add or Edit Inspect/Application FW Rule Wizard, Step 2

The options presented on the second page of the Inspect/Application FW Rule Wizard depend on your **Match Traffic By** selection on the first page (see Add or Edit Inspect/Application FW Rule Wizard, page 17-11). The possibilities are as follows:

- If you select Default Protocol Ports on the first page and *do not* select Limit inspection between source and destination IP addresses, the second page consists of the options described in Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17.
- If you select Default Protocol Ports on the first page and *do* select Limit inspection between source and destination IP addresses, the second page consists of the options described in the second table in this section. (The third page will consist of the options described in Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17.)
- If you select Custom Destination Ports on the first page, the second page consists of the options described in the first table in this section. (The third page will consist of the options described in Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17.)
- If you select Source and Destination Address and Port on the first page, the second page consists of the options described in the second table in this section. (The third page will consist of the options described in Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17.)

Navigation Path

From the Add or Edit Inspect/Application FW Rule Wizard, page 17-11, select a Match Traffic By option and click Next.

Related Topics

- Understanding Inspection Rules, page 17-2
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3
- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5
- Understanding Interface Role Objects, page 6-73
- Editing Rules, page 12-10

Field Reference

The following table describes the options presented on page 2 of the Inspect/Application FW Rule Wizard after you have selected **Custom Destination Ports** on the first page of the wizard (described in Add or Edit Inspect/Application FW Rule Wizard, page 17-11).

Table 17-3 Add and Edit Inspect/Application FW Rule Wizard Step 2: Protocol and Port Page

Element	Description
Protocol	The protocol for the ports you are specifying, either TCP, UDP, or both TCP/UDP. When configuring Custom Destination Ports for an IOS device, you must select TCP/UDP.
Ports	The port(s) used by the traffic you want to inspect. Valid values range from 1 to 65535. • Single—Specify one port number only. • Range—Specify a range of ports, for example, 10000-11000. When configuring custom ports, be aware that port ranges might not be supported on all platforms or OS versions. Any conflicts are identified during policy validation, not while you are editing this rule. **Tip** If you specify a port or port range that conflicts with a pre-defined port mapping, the device does not allow the port to be remapped.

The following table describes the options presented on page 2 of the Inspect/Application FW Rule Wizard after you have selected **Default Protocol Ports** and **Limit inspection between source and destination IP addresses** on the first page of the wizard, and when you select **Source and Destination Address and Port** on the first page. The first page of the wizard is described in Add or Edit Inspect/Application FW Rule Wizard, page 17-11.

Table 17-4 Add and Edit Inspect/Application FW Rule Wizard Step 2: Action, Sources, Destinations, and Services Page

Element	Description
Action	Whether you are identifying traffic that should be inspected based on the conditions set. Typically, you will create Permit rules. • Permit—Identifies traffic that will be inspected. • Deny—Exempts the traffic from inspection. Your access rules will determine if the traffic is allowed or blocked.

Table 17-4 Add and Edit Inspect/Application FW Rule Wizard Step 2: Action, Sources, Destinations, and Services Page (continued)

Element	Description
Sources	Provide traffic sources for this rule; can be networks, security groups, and users. You can enter values or object names, or Select objects, for one or more of the following types of sources: • Network – You can specify a various network, host and interface definitions, either individually or as objects. If you Select an interface object as a source, the dialog box displays tabs to differentiate between hosts/networks and interfaces. The "All-Address" objects do not restrict the rule to specific hosts, networks, or interfaces. These addresses are IPv4 or IPv6 addresses for hosts or networks, network/host objects, interfaces, or interface roles. **Note** You can only specify a fully qualified domain name (FQDN) by providing an FQDN network/host object, or a group object that includes an FQDN object. You cannot directly type in an FQDN. See Understanding Networks/Hosts Objects, page 6-80, Specifying IP Addresses During Policy Definition, page 6-87 and Understanding Interface Role Objects, page 6-73 for additional information about these definitions. • Security Groups (ASA 9.0+) – Enter or Select the name or tag number for one or more source security groups for the rule, if any. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups. • Users – Enter or Select the Active Directory (AD) user names, user groups, or identity user group objects for the rule, if any. You can enter any combination of the following: – Individual user names: NetBIOS_DOMAIN\username – User groups (note the double \): NetBIOS_DOMAIN\\user_group – Identity user group object names. For more information, see: – Selecting Identity Users in Policies, page 13-21 – Configuring Identity-Based Firewall Rules, page 13-21 – Creating Identity User Group Objects, page 13-19 **Note** Enter more than one value in any of these fields by separating the items with commas. Each specification is combined with any others to limit traffic matches to only those flows that include all definitions. For example, specified user traffic originating from within a specified source address range.

Table 17-4 Add and Edit Inspect/Application FW Rule Wizard Step 2: Action, Sources, Destinations, and Services Page (continued)

Element	Description
Destinations	Provide traffic destinations for this rule; can be networks or security groups. As with Sources, you can enter values or object names, or Select objects, for one or more destinations of Network and Security Group (ASA 9.0+) type.
Services	The services that define the type of traffic upon which to act. You can enter or Select any combination of service objects and service types (which are typically a protocol and port combination). Enter more than one value by separating the items with commas. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-100.
Time Range	The name of a time range policy object that defines the times when this rule applies. The time is based on the system clock of the device. The feature works best if you use NTP to configure the system clock. Enter the name or click **Select** to select the object. If the object that you want is not listed, click the **Create** button to create it.

Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page

Use the Inspect/Application FW Rule wizard's inspected protocol page to configure the protocol monitored by this inspection rule.

The options in this section are presented when you add or edit a firewall inspection rule, and when you right-click the Inspected Protocol cell of an existing rule in the table on the Inspection Rules Page, page 17-8.

Note Beginning with version 4.9, Security Manager supports SIP protocol for ASA cluster devices running the software version 9.4.0 or higher.

Navigation Path

Do one of the following:

- In the Add or Edit Inspect/Application FW Rule Wizard, page 17-11, click Next until you reach this page.
- To open the Edit Inspected Protocols dialog box, right-click the Inspected Protocol cell of an inspection rule and choose **Edit Inspected Protocol**. If you select multiple rows, your changes replace the inspected protocol defined for all selected rules.

Related Topics

- Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13
- Understanding Inspection Rules, page 17-2
- Choosing the Interfaces for Inspection Rules, page 17-2
- Selecting Which Protocols To Inspect, page 17-3

- Understanding Access Rule Requirements for Inspection Rules, page 17-4
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5
- Editing Rules, page 12-10
- Filtering Tables, page 1-48

Field Reference

Table 17-5 Inspected Protocol Options

Element	Description
Protocols table	Lists the protocols that can be inspected. You can select one protocol per rule. The list includes information on the device operating systems that allow inspection of the protocol: do not select protocols that are not supported by the device type to which you will apply the inspection rule. **Tip** For IOS devices, if you selected Custom Destination Ports or Destination Address and Port for the match type on the first page of the wizard, you can select **custom protocol** and click Configure to give your protocol a name. For other device types, select the protocol that you associate with the ports previously specified. The Options column displays configured options for the selected protocol, if any. The Group column provides additional information on the use of some of the protocols.
Selected Protocol Configure button	Displays the protocol you selected. If the protocol allows additional configuration, the Configure button becomes active; click it to see your options, and click the Help button in the dialog box that is opened for information about the options. For more information about protocols that allow configuration, see Configuring Protocols and Maps for Inspection, page 17-22.

Table 17-5 Inspected Protocol Options (continued)

Element	Description
Rule Settings (IOS)	Additional settings for the rule if it is used on devices running Cisco IOS software. If you select Use Default Inspection settings, the IOS defaults, or the settings defined in the inspection settings policy (see Configuring Settings for Inspection Rules for IOS Devices, page 17-111), are used. These are the settings you can enable or disable: • Alert—Whether to generate stateful packet inspection alert messages on the console. • Audit—Whether audit trail messages are logged to the syslog server or router. • Timeout—Whether to configure the length of time, in seconds, for which a session is managed while there is no activity. If you select Specify Timeout, enter the timeout value; the range is 5 to 43200 seconds. • Inspect Router Generated Traffic—Whether to inspect traffic that is generated by the device itself. This option is available for a limited number of the protocols.

Configure DNS Dialog Box

Use the Configure DNS dialog box to configure settings for DNS inspection on PIX 7.0+, ASA, FWSM, and IOS devices.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select DNS in the protocols table, and click **Configure**.

Field Reference

Table 17-6 Configure DNS Dialog Box

Element	Description
Maximum DNS Packet Length	The maximum DNS packet length. Values are 512 to 65535.
DNS Map	The DNS policy map object that defines traffic match conditions and actions, protocol conformance policies, and filter settings. Enter the object name, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.
Enable Dynamic Filter Snooping	Whether to allow the security appliance to snoop DNS packets in order to build a database of DNS lookup information. This information is used by botnet traffic filtering to match DNS names to IP addresses. If you configure a botnet traffic filtering rules policy, select this option. Otherwise, do not select the option. For more information, see Botnet Traffic Filter Rules Page, page 19-9.

Configure SMTP Dialog Box

Use the SMTP dialog box to edit settings for Simple Mail Transfer Protocol (SMTP) inspection. SMTP is used to transfer email between servers and clients on the Internet.

SMTP inspection drops any packets with illegal commands. You can configure a maximum data length for packets. Enter a length in the range 0-4294967295.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select SMTP in the protocols table, and click **Configure**.

Configure ESMTP Dialog Box

Use the Configure ESMTP dialog box to edit settings for Extended Simple Mail Transport Protocol (ESMTP) inspection. You can configure these settings based on platform:

- IOS devices—You can configure a maximum data length for packets. Enter a length in the range 0-4294967295.
- ASA/PIX 7.x+ devices—You can specify an ESMTP policy map object to define deep inspection parameters. Enter the name of the object or click **Select** to select it from a list or to create a new object.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select ESMTP in the protocols table, and click **Configure**.

Configure Fragments Dialog Box

Use the Configure Fragments dialog box to edit settings for fragment inspection on IOS devices.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select fragment in the protocols table, and click **Configure**.

Field Reference

Table 17-7 Configure Fragments Dialog Box

Element	Description
Maximum Fragments	The maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. Values are 0-10000 state entries. The default is 256. **Note** Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.

Table 17-7 Configure Fragments Dialog Box (continued)

Element	Description
Timeout (sec)	The number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. Values are 1-1000. The default timeout value is one second.

Configure IMAP or POP3 Dialog Boxes

Use the Configure IMAP or POP3 dialog boxes to edit settings for Internet Message Access Protocol (IMAP) or Post Office Protocol 3 (POP3) inspection on IOS devices.

- IMAP is a method for accessing electronic mail or bulletin board messages that are kept on a mail server that may be shared. It permits a client email program to access remote messages as though they were local.
- POP3 is used to receive email that is stored on a mail server. Unlike IMAP, POP retrieves mail only from a remote host.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select IMAP or POP3, and click **Configure**.

Field Reference

Table 17-8 Configure IMAP or POP3 Dialog Boxes

Element	Description
Reset Connection on Invalid IMAP/POP3 packet	Whether to reset, or drop, the connection between the client and server if an invalid packet is encountered. The client will have to repeat the validation process to reconnect to the server.
Enforce Secure Authentication	Whether to require that the client use a secure login to the server, that is, so that passwords are not sent in clear text.

Configure RPC Dialog Box

Use the RPC dialog box to edit settings for RPC inspection on IOS devices. RPC inspection blocks traffic for all RPC programs except for those you specify. To allow more than one RPC program, create a rule for each program number you want to allow.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select RPC in the protocols table, and click **Configure**.

Field Reference

Table 17-9 Configure RPC Dialog Box

Element	Description
Program Number	The program number to permit. Values are 1-4294967295.

Table 17-9 Configure RPC Dialog Box (continued)

Element	Description
Wait Time	The number of minutes to keep a hole in the firewall open to allow subsequent connections from the same source address to the same destination address and port. Values are 0-35791 minutes. The default is 0.

Custom Protocol Dialog Box

Use the Custom Protocol dialog box to assign a name to the protocol and port specification you made on the Add or Edit Inspect/Application FW Rule Wizard, Step 2, page 17-13 for IOS devices.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select custom protocol in the protocols table, and click **Configure**.

Configure Dialog Box

Use the Configure dialog box to select a policy map object for HTTP or IM inspection. The maps used for these types of inspection differ depending on the operating system version used on the device. Select the desired version and then click **Select** to select the desired policy map object or to create a new one.

Navigation Path

Go to the Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17, select HTTP or IM in the protocols table, and click **Configure**.

Configuring Protocols and Maps for Inspection

When you configure inspection rules for a device, you select the protocols that you want to inspect. Some of these protocols allow additional configuration for deep inspection. Deep inspection allows you to specify additional requirements that packets must meet in order to traverse the device. For example, you can drop HTTP connections where the content type of the request and response do not match. (For a full list of inspectible protocols, click **Add Row** on the Inspection Rule page and click Next to view the protocols list.)

What you can configure depends not only on the protocol but on the device's operating system and version number. Typically, your ability to fine-tune inspection is higher on an ASA device compared to an IOS device. (If you are configuring an IOS device and you want greater control over inspection, consider configuring zone-based firewall inspection; for more information, see Understanding the Zone-based Firewall Rules, page 21-3.)

Some deep inspection configuration is done directly in the inspection rule. However, for some protocols, you can configure the inspection rule to include a policy map that you create as an independent policy object. (You need to configure policy maps only if you want something other than the default inspection options.) You can configure these maps from the policy object selector dialog box while configuring the policy, or from the Policy Object Manager window (select **Manage > Policy Objects**).

For protocols that use policy maps, you can select the desired policy map, which defines the match conditions for the targeted traffic. For ASA, PIX, and FWSM devices, these policy maps might point to class maps that define the match conditions. To create these policy maps in the Policy Object Manager,

select one of the maps listed in the following table in the **Maps > Policy Maps > Inspect** folder and review the detailed usage information in the references mentioned. For information on creating class maps, which are in the **Maps > Class Maps > Inspect** folder, see the references to the match criterion dialog boxes and Configuring Class Maps for Inspection Policies, page 17-28.

Table 17-10 Configuring Protocols for Deep Inspection in Inspection Rules

Protocol	Device Types	Policy Map	Class Map (ASA, PIX, FWSM only)	Description and Match Criteria Reference
DNS	ASA, PIX, FWSM, IOS	DNS	DNS	Inspect traffic based on a wide variety of criteria using the class and policy map, which allow extensive control over DNS packets. In addition, you can configure a maximum length in the inspection rule, and enable dynamic DNS snooping for use with Botnet rules (on ASA devices). See the following topics: • Configuring DNS Maps, page 17-32 • DNS Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-36 • Configure DNS Dialog Box, page 17-19
FTP Strict	ASA, PIX, FWSM, IOS	FTP	FTP	Inspect traffic based on file name, type, server, user, or FTP command. See Configuring FTP Maps, page 17-42 and FTP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-43.
GTP	ASA, PIX, FWSM, IOS	GTP	GTP	Inspect traffic based on timeout values, message sizes, tunnel counts, and GTP versions traversing the security appliance. See Configuring GTP Maps, page 17-45 and GTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-49.

Table 17-10 Configuring Protocols for Deep Inspection in Inspection Rules (continued)

Protocol	Device Types	Policy Map	Class Map (ASA, PIX, FWSM only)	Description and Match Criteria Reference
H.323 H.225 H.323 RAS	ASA, PIX, FWSM	H.323 (ASA, PIX, FWSM)	H.323 (ASA, PIX, FWSM)	Inspect traffic based on a wide variety of criteria, including the H.323 message type, calling party, and called party. See Configuring H.323 Maps, page 17-51 and H.323 Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-54.
HTTP	ASA, PIX, FWSM, IOS	HTTP (ASA 7.1.x, PIX 7.1.x, FWSM 3.x, IOS) HTTP (ASA 7.2+, PIX 7.2+)	HTTP (ASA, PIX, FWSM)	Inspect traffic based on a wide variety of criteria including the content of the header or body, port misuse, and whether the traffic includes a Java applet. The maps used differ based on the operating system and version. **For ASA/PIX 7.2+**, see Configuring HTTP Maps for ASA 7.2+ and PIX 7.2+ Devices, page 17-64 and HTTP Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-66. **For ASA/PIX 7.1.x, FWSM 3.x+, and IOS**, see Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.
SIP	ASA, PIX, FWSM	SIP (ASA, PIX, FWSM)	SIP (ASA, PIX, FWSM)	Inspect traffic based on a wide variety of criteria. See Configuring SIP Maps, page 17-83 and SIP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-85.
Skinny	ASA, PIX, FWSM, IOS	Skinny	(none)	Inspect traffic based on a wide variety of criteria. See Configuring Skinny Maps, page 17-87 and Skinny Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-89.

Table 17-10 Configuring Protocols for Deep Inspection in Inspection Rules (continued)

Protocol	Device Types	Policy Map	Class Map (ASA, PIX, FWSM only)	Description and Match Criteria Reference
SMTP	ASA, PIX 7.x+, FWSM 3.x+, IOS	(none)	(none)	Inspect Simple Mail Transfer Protocol (SMTP) traffic and drop any that use illegal commands. You can configure a maximum data length for packets. See Configure SMTP Dialog Box, page 17-20.
SNMP	ASA, PIX, FWSM 3.x+, IOS	SNMP	(none)	Inspect SNMP traffic based on SNMP version. See Configuring SNMP Maps, page 17-90.
NetBIOS	ASA, PIX 7.x+, FWSM	NetBIOS	(none)	Inspect NetBIOS traffic to translate IP addresses in the NetBIOS name service (NBNS) packets according to the security appliance NAT configuration. You can drop packets that violate the protocol. See Configuring NetBIOS Maps, page 17-81.
IPSec Pass Through	ASA, PIX 7.x+	IPsec Pass Through	(none)	Inspect IPSec traffic and control whether ESP or AH traffic is allowed. See Configuring IPsec Pass Through Maps, page 17-80.
DCE/RPC	ASA 7.2+, PIX 7.2+, FWSM 3.2+	DCE/RPC	(none)	Inspect traffic based on timeouts and enforcing the mapper service. See Configuring DCE/RPC Maps, page 17-29.
IP options	ASA 8.2(2)+	IP Options	(none)	Allow IP packets that have certain options configured in the Options section of the IP header. In routed mode, packets that contain the router-alert option are allowed. Otherwise, if any option is set, packets are dropped. IP options are unnecessary for most communication, but the NOP (no operation) option might be used for padding, so you might want to allow it. See Configuring IP Options Maps, page 17-75.

Table 17-10 Configuring Protocols for Deep Inspection in Inspection Rules (continued)

Protocol	Device Types	Policy Map	Class Map (ASA, PIX, FWSM only)	Description and Match Criteria Reference
IPv6	ASA 8.4(2)+	IPv6	(none)	Inspect IPv6 traffic based on the following types of extension headers found anywhere in an IPv6 packet: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, and Encapsulating Security Payload. See Configuring IPv6 Maps, page 17-77 and IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-78.
ESMTP	ASA, PIX 7.x+, FWSM 3.x+, IOS	ESMTP	(none)	Inspect ESMTP traffic. For IOS, you can configure only maximum data length. For ASA, PIX, FWSM, you can inspect traffic based on a wide variety of criteria. See Configuring ESMTP Maps, page 17-39.
Fragment	IOS	(none)	(none)	Inspect traffic based on a maximum allowed number of unassembled packet fragments. See Configure Fragments Dialog Box, page 17-20.
IMAP (Internet Message Access Protocol) POP3 (Post Office Protocol 3)	IOS	(none)	(none)	Inspect traffic based on invalid commands or clear text logins. See Configure IMAP or POP3 Dialog Boxes, page 17-21.
RPC (Sun Remote Procedure Call)	FWSM 2.x, IOS	(none)	(none)	Inspect traffic based on the RPC protocol number. See Configure RPC Dialog Box, page 17-21.

Table 17-10 Configuring Protocols for Deep Inspection in Inspection Rules (continued)

Protocol	Device Types	Policy Map	Class Map (ASA, PIX, FWSM only)	Description and Match Criteria Reference
IM	ASA, PIX 7.x+, IOS	IM (ASA 7.2+, PIX 7.2+) IM (IOS)	IM (only for ASA, PIX)	Inspect traffic based on a wide variety of criteria. The allowed maps differ based on operating system version. **For ASA, PIX**, see Configuring IM Maps for ASA 7.2+, PIX 7.2+ Devices, page 17-70 and IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-71. **For IOS**, see Configuring IM Maps for IOS Devices, page 17-73.
SCTP	ASA 9.5(2)+	SCTP	(none)	Inspect traffic based on Payload PID (PPID). See Configuring SCTP Maps, page 17-91 and SCTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-92
Diameter	ASA 9.5(2)+	Diameter	Diameter	Inspect traffic based on application ID, command codes, and AVP. See Configuring Diameter Maps, page 17-93 and Diameter Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-95
LISP	ASA 9.5(2)+	LISP	None	Inspect traffic allowed Endpoint Identifiers access list and validation key. See Configuring LISP Maps, page 17-102
M3UA	ASA 9.6(2)+	M3UA	None	Drops and logs packets that do not meet M3UA protocol conformance. See Configuring M3UA Maps, page 17-103

Related Topics

- Selecting Which Protocols To Inspect, page 17-3
- Understanding Inspection Rules, page 17-2
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5
- Configuring Inspection Rules, page 17-5
- Creating Policy Objects, page 6-9

- Understanding Map Objects, page 6-78
- Add/Edit Regular Expressions, page 17-108
- Configuring Regular Expression Groups, page 17-108

Configuring Class Maps for Inspection Policies

Use the Add and Edit Class Map dialog boxes to define class maps to be used in policy maps of the same type. The name of the dialog box indicates the type of map you are creating.

A class map defines application traffic based on criteria specific to the application. You then select the class map in the corresponding policy map and configure the action to take for the selected traffic. Thus, each class map must contain traffic that you want to handle in the same way (for example, to allow it or to drop it).

When configuring inspection rules for devices running ASA/PIX 7.2 or higher, or FWSM, you can create class maps for the inspection of the following types of traffic: DNS, FTP, H.323, HTTP, IM, SIP, and ScanSafe.

You can also define class criteria in the related policy map. However, creating class maps allows you to reuse the map in multiple policy maps.

The following topics describe the available match criteria:

- DNS Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-36
- FTP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-43
- H.323 Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-54
- HTTP Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-66
- IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-71
- SIP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-85
- Diameter Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-95

Navigation Path

Select **Manage > Policy Objects**, then select DNS, FTP, H.323 (ASA/PIX/FWSM), HTTP (ASA/PIX/FWSM), IM, SIP (ASA/PIX/FWSM), Diameter in the **Maps > Class Maps > Inspect** folder in the table of contents. Right-click inside the work area, then select **New Object**, or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Understanding Inspection Rules, page 17-2

Field Reference

Table 17-11 Add or Edit Class Maps Dialog Boxes for Inspection Rules

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Match table Match Type	The Match table lists the criteria included in the class map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion and the criterion and value that is inspected. • To add a criterion, click the Add button and fill in the Match Criterion dialog box. For more information, see the topics referenced above. • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring DCE/RPC Maps

Use the Add or Edit DCE/RPC Map dialog boxes to define a map for DCE/RPC inspection. A DCE/RPC inspection policy map lets you change the default configuration values used for DCE/RPC inspection.

DCE/RPC 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.

DCE/RPC 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. Because a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have user configurable timeouts.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > DCE/RPC** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-12 Add and Edit DCE/RPC Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Pinhole Timeout	The timeout for DCE/RPC pinholes. The default is 2 minutes (00:02:00). Valid values are between 00:00:01 and 1193:00:00.
Enforce Endpoint Mapper Service	Whether to enforce the endpoint mapper service during binding. Using this service, a client queries a server, called the Endpoint Mapper, for the dynamically allocated network information of a required service.
Enable Endpoint Mapper Service Lookup Service Lookup Timeout	Whether to enable the lookup operation of the endpoint mapper service. If you select this option, you can enter the time out for the lookup operation. If you do not specify a timeout, the pinhole timeout or default pinhole timeout value is used. Valid values are between 00:00:01 and 1193:00:00.
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see DCE/RPC Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-31). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

DCE/RPC Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit DCE/RPC Match Criterion (for DCE/RPC class maps) or Match Condition and Action (for DCE/RPC policy maps) dialog boxes to do the following:

- Define the match criterion and value for a DCE/RPC class map.
- Select a DCE/RPC class map when creating a DCE/RPC policy map.
- Define the match criterion, value, and action directly in a DCE/RPC policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating a DCE/RPC class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for DCE/RPC, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating a DNS policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit DNS Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring DCE/RPC Maps, page 17-29.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-13 DCE/RPC Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing DCE/RPC class map or define a new DCE/RPC class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing DCE/RPC class map policy object. Enter the name of the DNS class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of traffic to match: • ms-rpc-epm—Matches Microsoft RPC EPM messages. • ms-rpc-isystemactivator—Matches ISystemMapper messages. • ms-rpc-oxidresolver-—Matches OxidResolver messages.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.

Table 17-13 DCE/RPC Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria. • Reset—Drop the packet, close the connection, and send a TCP reset to the server or client. • Log—Send a system log message. You can use this option alone or with one of the other actions. • Reset and Log— Perform the reset and log actions.

Configuring DNS Maps

Use the Add and Edit DNS Map dialog boxes to define DNS Maps for inspection. A DNS map lets you change the default configuration values used for DNS application inspection.

DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. You can configure rules for certain DNS types to be allowed, dropped, or logged, while others are blocked. For example, you can restrict zone transfer between servers.

The Recursion Desired and Recursion Available flags in the DNS header can be masked to protect a public server from attack if that server only supports a particular internal zone. In addition, DNS randomization can be enabled to avoid spoofing and cache poisoning of servers that either do not support randomization or that use a weak pseudo random number generator. Limiting the domain names that can be queried protects the public server further.

You can configure a DNS mismatch alert as notification if an excessive number of mismatching DNS responses are received, which could indicate a cache poisoning attack.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > DNS** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-14 Add and Edit DNS Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.

Table 17-14 Add and Edit DNS Map Dialog Boxes (continued)

Element	Description
Protocol Conformance Tab	
	Defines DNS security settings and actions. For a description of the options on this tab, see DNS Map Protocol Conformance Tab, page 17-33.
Filtering Tab	
	Defines the filtering settings for DNS. For a description of the options on this tab, see DNS Map Filtering Tab, page 17-34.
Mismatch Rate Tab	
	The **Log When DNS ID Mismatch Rate Exceeds** option determines whether you want to report excessive instances of DNS identifier mismatches based on the following criteria: • Threshold—The maximum number of mismatch instances before a system message log is sent. Values are 0 to 4294967295. • Time Interval—The time period to monitor (in seconds). Values are 1 to 31536000.
Umbrella Connector Tab	
	Defines DNS umbrella connector settings for a DNS. For a description of the options on this tab, see DNS Umbrella Connector Tab, page 17-35.
Match Condition and Action Tab	
	The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see DNS Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-36). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

DNS Map Protocol Conformance Tab

Use the Protocol Conformance tab to define DNS security settings and actions for a DNS map.

Navigation Path

Click the Protocol Conformance tab on the Add and Edit DNS Map dialog boxes. See Configuring DNS Maps, page 17-32.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-15 DNS Map Protocol Conformance Tab

Element	Description
Enable DNS Guard Function	Whether to perform a DNS query and response mismatch check using the identification field in the DNS header. One response per query is allowed to go through the security appliance.
Generate Syslog for ID Mismatch	Whether to create syslog entries for excessive instances of DNS identifier mismatches.
Randomize the DNS Identifier for DNS Query	Whether to randomize the DNS identifier in the DNS query message.
Enable NAT Rewrite Function	Whether to enable IP address translation in the A record of the DNS response.
Enable Protocol Enforcement	Whether to enable DNS message format check, including domain name, label length, compression, and looped pointer check.
Enable DNS on TCP	Whether to enable inspection of DNS over TCP traffic.Ensure that DNS/TCP port 53 traffic is part of the class to which you apply DNS inspection. The inspection default class includes TCP/53.
Require Authentication Between DNS Server (RFC2845) Action	Whether to require authentication between DNS servers as defined in RFC 2845. If you select this option, select the action to take when there is no authentication.

DNS Map Filtering Tab

Use the Filtering tab to define DNS filtering settings and actions for a DNS map.

Navigation Path

Click the Filtering tab on the Add and Edit DNS Map dialog boxes. See Configuring DNS Maps, page 17-32.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-16 DNS Map Filtering Tab

Element	Description
Drop Packets that Exceed Specified Length Maximum Packet Length	Whether to drop packets that exceed the maximum length in bytes that you specify. This is a global setting.
Drop Packets Sent to Server that Exceed Specified Maximum Length Maximum Length	Whether to drop packets sent to the server that exceed the maximum length in bytes that you specify.
Drop Packets Sent to Server that Exceed Length Indicated by Resource Record	Whether to drop packets sent to the server that exceed the length indicated by the resource record.
Drop Packets Sent to Client that Exceed Specified Length Maximum Length	Whether to drop packets sent to a client that exceed the maximum length in bytes that you specify.
Drop Packets Sent to Client that Exceed Length Indicated by Resource Record	Whether to drop packets sent to the client that exceed the length indicated by the resource record.

DNS Umbrella Connector Tab

Use the Umbrella Connector tab to define DNS umbrella connector settings for a DNS map. Beginning with Cisco Security Manager version 4.18, the Umbrella global policy is supported on ASA 9.10.1 devices and above.

Navigation Path

Click the Umbrella Connector tab on the Add and Edit DNS Map dialog boxes. See Configuring DNS Maps, page 17-32.

Related Topics

- Configuring Umbrella Global Policy, page 48-16

Field Reference

Table 17-17 DNS Umbrella Connector Tab

Element	Description
Enable Umbrella Connector Tag for Umbrella Policy	Select the check box and enter the DNS policy-map umbrella tag name. The tag name can be a maximum of 50 characters. Cisco Security manager throws an error message if the tag name is greater than 50 characters. **Note** If the Umbrella global policy is not configured, Cisco Security Manager displays activity validation error. For more information on Umbrella global policy configuration, see Configuring Umbrella Global Policy, page 48-16.

Table 17-17 DNS Umbrella Connector Tab (continued)

Element	Description
Enable DNScrypt	Select this check box to enable the DNS crypt in the Umbrella datapath. For every hour, the secret key is exchanged between the key exchange thread and the Umbrella resolver. Ensure that the **Enable Umbrella Connector** check box is selected. If the check box is not selected, an error message is displayed for configuration discrepancy. **Note** If the Umbrella global policy is not configured, Cisco Security Manager displays activity validation error. For more information on Umbrella global policy configuration, see Configuring Umbrella Global Policy, page 48-16.

DNS Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit DNS Match Criterion (for DNS class maps) or Match Condition and Action (for DNS policy maps) dialog boxes to do the following:

- Define the match criterion and value for a DNS class map.
- Select a DNS class map when creating a DNS policy map.
- Define the match criterion, value, and action directly in a DNS policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating a DNS class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for DNS, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating a DNS policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit DNS Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring DNS Maps, page 17-32.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-18 DNS Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing DNS class map or define a new DNS class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing DNS class map policy object. Enter the name of the DNS class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of traffic to match: • DNS Class—Matches a DNS query or resource record class. • DNS Type—Matches a DNS query or resource record type. • Domain Name—Matches a domain name from a DNS query or resource record. • Header Flag—Matches a DNS flag in the header. • Question—Matches a DNS question. • Resource Record—Matches a DNS resource record.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Value (for DNS Class criterion)	The DNS class you want to inspect: • Internet—Matches the Internet DNS class. • DNS Class Field Value—Matches the specified number. • DNS Class Field Range—Matches the specified range of numbers.

Table 17-18 DNS Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Value (for DNS Type criterion)	The DNS type you want to inspect: • DNS Type Field Name—Matches the name of a DNS type: – 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. – TSIG—Transaction signature. • DNS Type Field Value—Matches the specified number. • DNS Type Field Range—Matches the specified range of numbers.
Value (for Domain Name criterion)	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
Options Value (for Header Flag criterion)	The header flag you want to inspect. Use the Options field to indicate whether you want an exact match (Equals) or a partial match (Contains). • Header Flag Name—Matches the selected header flag names: – AA (authoritative answer) – QR (query) – RA (recursion available) – RD (recursion denied) – TC (truncation) flag bits • Header Flag Value—Matches the specified 16-bit hexadecimal value.
Resource Record	Lists the sections to match: • Additional—DNS additional resource record. • Answer—DNS answer resource record. • Authority—DNS authority resource record.

Configuring ESMTP Maps

Use the Add and Edit ESMTP Map dialog boxes to define the match criterion and values for the ESMTP inspect map. An ESMTP policy map lets you change the default configuration values used for ESMTP inspection.

ESMTP inspection detects attacks, including spam, phising, malformed message attacks, and buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detect several attacks, block senders/receivers, and block mail relay.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > ESMTP** from the Object Type selector. Right-click inside the table, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-19 Add and Edit ESMTP Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Mask Server Banner	Whether to mask the server banner to prevent the client from discovering server information.
Configure Mail Relay Domain Name Action	Whether to have ESMTP inspection detect mail relay. When you select this option, enter the domain name you are inspecting and select the action you want to take when mail relay is detected.
Special Character (ASA7.2.3+/PIX7.2.3+) Action	Whether you want to detect special characters in sender or receiver email addresses. If you select this option, select the action you want to take when special characters are detected.
Allow TLS (ASA7.2.3+, 8.0.3+/PIX7.2.3) Action Log	Whether to allow a TLS proxy on the security appliance. If you select this option, you can also select Action Log to create a log entry when TLS is detected.

Table 17-19 Add and Edit ESMTP Map Dialog Boxes (continued)

Element	Description
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see ESMTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-40). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

ESMTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Add or Edit Match Condition and Action dialog boxes to define the match criterion, value, and action for an ESMTP policy map.

The fields on this dialog box change based on the criterion you select. You can use the following criteria:

- Body Length—Matches the message body length.
- Body Line Length—Matches the length of a line in the message body.
- Commands—Matches ESMTP commands.
- Command Recipient Count—Matches the number of recipient email addresses.
- Command Line Length—Matches the number of characters of a command line.
- EHLO Reply Parameters—Matches the ESMTP EHLO reply parameters.
- Header Length—Matches the number of characters of the header.
- Header Line Length—Matches the number of characters of a line in the message header.
- To Recipients Count—Matches the number of recipients in the To field of the header.
- Invalid Recipients Count—Matches the number of invalid recipients in the header.
- MIME File Type—Matches the MIME file type.
- MIME Filename Length—Matches the number of characters of the filename.
- MIME Encoding—Matches the MIME encoding scheme.
- Sender Address—Matches the address of the sender.
- Sender Address Length—Matches the number of characters of the sender's address.

Navigation Path

In the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit ESMTP Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring ESMTP Maps, page 17-39.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-20 ESMTP Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Specifies which criterion of ESMTP traffic to match. The criteria are described above.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action	The action you want the device to take for traffic that matches the defined criteria.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Greater Than Length	The length in bytes of the evaluated field. The criterion matches if the length is greater than the specified number, and does not match if the field is less than the specified number. The dialog box indicates the valid range for the length, except for Body Length and Header length, which can be 1 to 4294967295.
Commands	The ESMTP command verbs you want to inspect.
Greater Than Count	The number of evaluated items. The criterion matches if the count is greater than the specified number, and does not match if the count is less than the specified number.
Parameters	The ESMTP EHLO reply parameters you want to inspect.

Table 17-20 ESMTP Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
MIME Encoding	The type of MIME encoding schemes you want to inspect.

Configuring FTP Maps

Use the Add and Edit FTP Map dialog boxes to define the match criterion and values for an FTP inspect map. You can use an FTP map to block specific FTP protocol methods, such as an FTP PUT, from passing through the security appliance and reaching your FTP server.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > FTP** from the Object Type selector. Right-click inside the table, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-21 Add and Edit FTP Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Mask Greeting Banner from Server	Whether to mask the greeting banner from the FTP server to prevent the client from discovering server information.
Mask Reply to SYST Command	Whether to mask the reply to the **syst** command to prevent the client from discovering server information.

Table 17-21 Add and Edit FTP Map Dialog Boxes (continued)

Element	Description
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see FTP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-43). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.
Validate For Validate button	The device platforms for which to validate the object. Select the platform for which you intend to use this object and click **Validate** to determine if the object is configured in a way that will prevent policy deployment.

FTP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit FTP Match Criterion (for FTP class maps) or Match Condition and Action (for FTP policy maps) dialog boxes to do the following:

- Define the match criterion and value for an FTP class map.
- Select an FTP class map when creating an FTP policy map.
- Define the match criterion, value, and action directly in an FTP policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating an FTP class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for FTP, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating an FTP policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit FTP Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring FTP Maps, page 17-42.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-22 FTP Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing FTP class map or define a new FTP class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing FTP class map policy object. Enter the name of the FTP class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of FTP traffic to match: • Request Command—Matches an FTP request command. • Filename—Matches a filename for FTP transfer. • File Type—Matches a file type for FTP transfer. • Server—Matches an FTP server name. • Username—Matches an FTP username.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.

Variable Fields

The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.

Table 17-22 FTP Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Request Commands	The FTP commands you want to inspect: • Append (APPE)—Appends to a file. • Delete (DELE)—Deletes a file at the server site. • Help (HELP)—Provides help information from the server. • Put (PUT)—FTP client command for the stor (store a file) command. • Rename From (RNFR)—Specifies rename-from filename. • Server Specific Command (SITE)—Specifies commands that are server specific. Usually used for remote administration. • Change to Parent (CDUP)—Changes to the parent directory of the current working directory. • Get (GET)—FTP client command for the retr (retrieve a file) command. • Create Directory (MKD)—Creates a directory. • Remove Directory (RMD)—Removes a directory. • Rename To (RNTO)—Specifies rename-to filename. • Store File with Unique Name (STOU)—Stores a file with a unique filename.
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.

Configuring GTP Maps

Use the Add and Edit GTP Map dialog boxes to define the match criterion and values for a GTP inspect map.

The GPRS Tunnel Protocol (GTP) provides uninterrupted connectivity for mobile subscribers between GSM networks and corporate networks or the Internet. GTP uses a tunneling mechanism to provide a service for carrying user data packets.

A GTP map object lets you change the default configuration values used for GTP application inspection. The GTP protocol is designed to provide security for wireless connections to TCP/IP networks such as the Internet. You can use a GTP map to control timeout values, message sizes, tunnel counts, and GTP versions traversing the security appliance.

Starting from version 4.18, Cisco Security Manager supports anti-replay feature of ASA 9.10.1. By enabling data packet replay, your network is protected from replay attacks.

Tip GTP inspection requires a special license. If you do not have the required license, you will see device errors if you try to deploy a GTP map.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > GTP** from the Object Type selector. Right-click inside the work area, then select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-23 Add and Edit GTP Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Country and Network Codes Table	The three-digit Mobile Country Code (mcc) and Mobile Network Code (mnc) to include in the map. The codes are 000 to 999. • To add codes, click the Add button and fill in the dialog box. • To edit a row, select it and click the Edit button. • To delete a row, select it and click the Delete button.
Permit Response Table	The Network/Host policy objects for which you will allow GTP responses from a GSN that is different from the one to which the response was sent. • To add objects, click the Add button and fill in the dialog box. For more information, see Add and Edit Permit Response Dialog Boxes, page 17-48. • To edit a row, select it and click the Edit button. • To delete a row, select it and click the Delete button.
Request Queue	The maximum requests allowed in the queue. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. Values are 1-9999999. The default is 200.

Table 17-23 Add and Edit GTP Map Dialog Boxes (continued)

Element	Description
Tunnel Limit	The maximum number of tunnels allowed.
Permit Errors	Whether to permit packets with errors or different GTP versions. By default, all invalid packets or packets that failed during parsing are dropped.
Enable Data Packet Replay Window	Select the check box to configure the anti-replay and select one of the four window sizes—128, 256, 512, or 1024. Messages that are outside of the window size are dropped. For information on configuration of GTP Map policy, refer to Add or Edit Inspect/Application FW Rule Wizard, Inspected Protocol Page, page 17-17.
Enable Header	Check Select the check box to enable header check of the data packets.
Anti-User Spoofing	This field is enabled only when you select the Enable Header Check check box. Select the relevant option: • Bypass—to forward the packets that pass the header check. • Drop—to drop the packets that pass the header check.
Edit Timeouts button	Click this button to configure time out values for various operations. For more information about the options, see GTP Map Timeouts Dialog Box, page 17-48.

Match Condition and Action Tab

The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions.

- To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see GTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-49).
- To edit a criterion, select it and click the Edit button.
- To delete a criterion, select it and click the Delete button.

Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.
Validate For Validate button	The device platforms for which to validate the object. Select the platform for which you intend to use this object and click **Validate** to determine if the object is configured in a way that will prevent policy deployment.

Add and Edit Country Network Codes Dialog Boxes

Use the Add and Edit Country Network Codes dialog boxes to add Mobile Country Code (mcc) and Mobile Network Code (mnc) values to the GTP policy map. The codes can be 000 to 999.

Navigation Path

From the Add and Edit GTP Map dialog boxes, click the **Add** button in the Country and Network codes table, or select a row and click the **Edit** button. See Configuring GTP Maps, page 17-45.

Add and Edit Permit Response Dialog Boxes

Use the Add and Edit Permit Response dialog boxes to permit GTP responses from a GSN that is different from the one to which the response was sent.

Enter the name of a Network/Host policy object that defines the destination (**To Object Group**) and source (**From Object Group**) of the traffic. You can click **Select** to select the object from a list, where you can also create an new object by clicking the **Create** button in the Object Selector dialog box.

You cannot use the Network/Host object named “any.”

Navigation Path

From the Add and Edit GTP Map dialog boxes, click the **Add** button in the Permit Response table, or select a row and click the **Edit** button. See Configuring GTP Maps, page 17-45.

GTP Map Timeouts Dialog Box

Use the GTP Map Timeouts dialog box to set timeout values for a GTP Map.

Navigation Path

From the Add and Edit GTP Map dialog boxes, click the **Edit Timeouts** button on the Parameters tab. See Configuring GTP Maps, page 17-45.

Field Reference

Table 17-24 GTP Map Timeouts Dialog Box

Element	Description
GSN Timeout (Prior to ASA 9.5(1)) Endpoint Timeout (ASA 9.5(1) or higher)	The period of inactivity (hh:mm:ss) after which a GSN is removed. The default is 30 minutes. Enter 0 to never tear down immediately.
PDP Context Timeout	The maximum period of time allowed (hh:mm:ss) before beginning to receive the PDP context. The default is 30 minutes. Enter 0 to specify no limit.
Request Queue Timeout	The maximum period of time allowed (hh:mm:ss) before beginning to receive the GTP message. The default is 60 seconds. Enter 0 to specify no limit.
Signaling Connections Timeout	The period of inactivity (hh:mm:ss) after which the GTP signaling is removed. The default is 30 minutes. Enter 0 to not remove the signal.

Table 17-24 GTP Map Timeouts Dialog Box (continued)

Element	Description
Tunnel Timeout	The period of inactivity (hh:mm:ss) after which the GTP tunnel is torn down. The default is 60 seconds (when a Delete PDP Context Request is not received). Enter 0 to never tear down immediately.
T3 Response Timeout	The maximum wait time for a response before removing the connection.

GTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Add or Edit Match Condition and Action dialog boxes to define the match criterion, value, and action for a GTP policy map.

The fields on this dialog box change based on the criterion you select.

Navigation Path

In the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit GTP Map dialog box, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring GTP Maps, page 17-45.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-25 GTP Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Specifies which criterion of GTP traffic to match: • Access Point Name—Matches the access point name so you can define the access points to drop when GTP application inspection is enabled. • Message ID—Matches the numeric identifier for the message that you want to drop. By default, all valid message IDs are allowed. • Message Length—Matches the length of the UDP packet. Use this criterion to change the default for the maximum allowed message length for the UDP payload. • Version—Matches the GTP version. • MSISDN—Matches the MSISDN with regular expressions or class and drop all GTP packets that have matching MSISDN. • Selection Mode—Ranges between 0 and 3.

Table 17-25 GTP Policy Maps Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action	The action you want the device to take for traffic that matches the defined criteria. • Drop Packet—By default, all invalid packets or packets that failed during parsing are dropped. • Drop Packet and Log • Rate Limit
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Access Point Name	The access points to act on when GTP application inspection is enabled. • Specified By—An access point name to be dropped. By default, all messages with valid APNs are inspected, and any APN is allowed. • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
ID type	The numeric identifier of the message that you want to act on. • Value—A single message ID. The Value can be between 1 and 255. • Range—A range of message IDs. The Range can be between 1 and 255.
Minimum Length	The minimum number of bytes in the UDP payload.
Maximum Length	The maximum number of bytes in the UDP payload.

Table 17-25 GTP Policy Maps Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Version	Beginning with version 4.9, Security Manager provides support for GPRS Tunnel Protocol (GTP) v2 and enhanced v1 in the GTP Map Object for ASA devices 9.5(1) or higher. You can now configure separate message ID matching for GTPv1 and GTPv2. For ASA devices 9.5(1) or higher, if you select Message ID as the Criterion, two options for Version, v1 and v2, are displayed. Select v1 or v2 and enter a single Value between 1 and 255, or a Range of values from 1 to 255.
Version Type	Prior to ASA version 9.5(1)—Use 0 to identify Version 0 and 1 to identify Version 1. Version 0 of GTP uses port 2123, while Version 1 uses port 3386. By default all GTP versions are allowed.
Regular Expression	Beginning with version 4.18, Cisco Security Manager allows configuring of MSISDN with regular expressions and drop all GTP packets that have matching MSISDN. This field appears when you select MSISDN in the Criterion drop-down.
Regular Expression Group	Beginning with version 4.18, Cisco Security Manager allows configuring of MSISDN with regular expressions class and drop all GTP packets that have matching MSISDN. This field appears when you select MSISDN in the Criterion drop-down.
Mode Value	If Selection is selected in the Criterion drop-down, this field appears. Enter the mode value in the range of 0 – 3. This is a mandatory field.

Configuring H.323 Maps

Use the Add and Edit H.323 Map dialog boxes to define the match criterion and values for an H.323 inspect map. An H.323 policy map lets you change the default configuration values used for H.323 inspection.

H.323 inspection supports H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The security appliance supports H.323 through Version 4, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the security appliance. The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.
- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > H.323 (ASA/PIX/FWSM)** from the Object Type selector. Right-click inside the work area, then select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-26 Add and Edit H.323 Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
HSI Group table	The HSI groups to include in the map. The group number, IP address of the HSI host, and IP addresses and interface names of the clients connected to the security appliance are shown in the table. Up to five HSI hosts per group, and up to ten end points per HSI group, are allowed. • To add a group, click the Add button and fill in the dialog box (see Add or Edit HSI Group Dialog Boxes, page 17-53). • To edit a group, select it and click the Edit button. • To delete a group, select it and click the Delete button.
Call Duration Limit	The call duration limit in seconds. The range is from 0:0:0 to 1163:0:0. A value of 0 means never timeout.
Enforce Presence of Calling and Called Party Numbers	Whether to enforce calling and called party numbers used in call setup.
Allow the facility message before SETUP for H.460.18	Whether to allow the FACILITY message to be sent before the SETUP message as part of the Incoming Call Message Procedure. **Note** H.460.18 defines a method for traversal of H.323 signaling across network address translators and firewalls.
Check State Transition on H.225 Messages	Whether to enable state checking validation on H.225 messages.
Check State Transition on RAS Messages	Whether to enable state checking validation on RAS messages.
Create Pinholes on Seeing RCF Packets	Whether to enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The device opens pinholes for calls based on Registration Request/Registration Confirm (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 device opens a pinhole through source IP address/port 0/0. This option is available for ASA 8.0(5)+ devices.
Check for H.245 Tunneling Action	Whether to enforce H.245 tunnel blocking and perform the action you select in the Action list box.

Table 17-26 Add and Edit H.323 Map Dialog Boxes (continued)

Element	Description
Check RTP Packets for Protocol Conformance	Whether to check RTP packets flowing through the pinholes for protocol conformance.
Payload Type must be Audio or Video based on Signaling Exchange	Whether to enforce the payload type to be audio or video based on the signaling exchange.

Match Condition and Action Tab

The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions.

- To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see H.323 Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-54).
- To edit a criterion, select it and click the Edit button.
- To delete a criterion, select it and click the Delete button.

Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit HSI Group Dialog Boxes

Use the Add or Edit HSI group dialog boxes to add HSI groups to an H.323 policy inspection map.

Navigation Path

From the Parameters tab on the Add and Edit H.323 Map dialog boxes, click the **Add Row** button in the HSI group table, or select a row and click the **Edit Row** button. See Configuring H.323 Maps, page 17-51.

Field Reference

Table 17-27 Add and Edit HSI Group Dialog Boxes

Element	Description
Group ID	The HSI group ID number (0 to 2147483647).
IP Address	The IP address of the HSI host.

Table 17-27 Add and Edit HSI Group Dialog Boxes (continued)

Element	Description
Endpoint table	The end points associated with HSI group. You can add up to 10 end points per group. For each end point, you specify the IP address and interface policy group. • To add an end point, click the Add button and fill in the dialog box (see Add or Edit HSI Endpoint IP Address Dialog Boxes, page 17-54). • To edit an end point, select it and click the Edit button. • To delete an end point, select it and click the Delete button.

Add or Edit HSI Endpoint IP Address Dialog Boxes

Us the Add or Edit HSI Endpoint IP Address dialog box to add end points to an HSI group.

Navigation Path

From the Add and Edit HSI Group dialog boxes, click the **Add Row** button in the end point table, or select a row and click the **Edit Row** button. See Configuring H.323 Maps, page 17-51.

Field Reference

Table 17-28 Add and Edit HSI Endpoint IP Address Dialog Boxes

Element	Description
Network/Host	The IP address of the end point host or network.
Interface	The Interface policy group that identifies the interface connected to the security appliance. Enter the name of a policy group, or click **Select** to select it from a list, where you can also create new policy groups.

H.323 Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit H.323 Match Criterion (for H.323 class maps) or Match Condition and Action (for H.323 policy maps) dialog boxes to do the following:

- Define the match criterion and value for an H.323 class map.
- Select an H.323 class map when creating an H.323 policy map.
- Define the match criterion, value, and action directly in an H.323 policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating an H.323 class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for H.323, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating an H.323 policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit H.323 Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring H.323 Maps, page 17-51.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-29 H.323 Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing H.323 class map or define a new H.323 class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing H.323 class map policy object. Enter the name of the H.323 class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of H.323 traffic to match: • Called Party—Matches the called party address. • Calling Party—Matches the calling party address. • Media Type—Matches the media type.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
Media Type	The type of media you want to inspect, audio, video, or data.

Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX, FWSM, and IPS features/functionality, it does not support any enhancements.

Use the Add and Edit HTTP Map dialog boxes to define HTTP maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x, and IOS devices.

The enhanced HTTP inspection feature, which is also known as an application firewall, verifies that HTTP messages conform to RFC 2616, use RFC-defined methods, and comply with various other criteria. This can help prevent attackers from using HTTP messages for circumventing network security policy.

When you enable HTTP inspection with an HTTP map, strict HTTP inspection with the action reset and log is enabled by default. You can change the actions performed in response to inspection failure, but you cannot disable strict inspection as long as the HTTP map remains enabled. Security Manager uses the **http-map** command to configure the map on the device.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > HTTP (ASA 7.1.x/PIX 7.1.x/FWSM3.x/IOS)** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-30 Add and Edit HTTP Map Dialog Boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
General tab	Defines the action taken when non-compliant HTTP requests are received and to enable verification of content type. For a description of the options, see HTTP Map General Tab, page 17-57.
Entity Length tab	Defines the action taken if the length of the HTTP content falls outside of configured targets. For a description of the options, see HTTP Map Entity Length Tab, page 17-58.
RFC Request Method tab	Defines the action that the security appliance should take when specific RFC request methods are used in the HTTP request. For a description of the options, see HTTP Map RFC Request Method Tab, page 17-60.
Extension Request Method tab	Defines the action taken when specific extension request methods are used in the HTTP request. For a description of the options, see HTTP Map Extension Request Method Tab, page 17-61.

Table 17-30 Add and Edit HTTP Map Dialog Boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices

Element	Description
Port Misuse tab	Defines the action taken when specific undesirable applications are encountered. For a description of the options, see HTTP Map Port Misuse Tab, page 17-62.
Transfer Encoding tab	Defines the action taken when specific transfer encoding types are used in the HTTP request. For a description of the options, see HTTP Map Transfer Encoding Tab, page 17-63.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

HTTP Map General Tab

Use the General tab to define the action taken when non-compliant HTTP requests are received and to enable verification of content type.

Navigation Path

Click the General tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-31 HTTP Map General Tab

Element	Description
Take action for non-RFC 2616 compliant traffic	Whether you want to configure the action to be taken for traffic that does not comply with RFC 2616. Possible actions are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server. You can also select **Generate Syslog** to write a message to the syslog if non-compliant traffic is encountered.

Table 17-31 HTTP Map General Tab (continued)

Element	Description
Verify Content-type field belongs to the supported internal content-type list.	Whether you want to configure the action to be taken for traffic whose content type does not belong to the supported internal content-type list. Possible actions are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server. You can also select these options: • **Verify Content-type field for response matches the ACCEPT field of request**—To also verify that the content type of the response matches the request. • **Generate Syslog**—To write a message to the syslog if non-compliant traffic is encountered.
Override Global TCP Idle Timeout (IOS only)	Whether to change the TCP idle timeout default setting. An IOS device terminates a connection if there is no communication activity after this length of time. If you select this option, specify the desired timeout value in seconds.
Override Global Audit Trail Setting (IOS only) Enable Audit Trail	Whether to change the audit trail setting for IOS devices. If you select this option, you can select **Enable Audit Trail** to generate audit trail messages.

HTTP Map Entity Length Tab

Use the Entity Length tab to enable inspection based on the length of the HTTP content.

Navigation Path

Click the Entity Length tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-32 HTTP Map Entity Length Tab

Element	Description
Inspect URI Length	Whether to enable inspection based on the length of the URI. If you select this option, configure the following: • Maximum—The desired maximum length, in bytes, of the URI, from 1 to 65535. • Excessive URI Length Action—The action to take when the length is exceeded: – Allow Packet—Allow the message. – Drop Packet—Close the connection. – Reset Connection—Send a TCP reset message to client and server. • Generate Syslog—Whether to generate a syslog message when a violation occurs.
Inspect Maximum Header Length	Whether to enable inspection based on the length of the HTTP header. If you select this option, configure the following: • Request—The desired maximum length, in bytes, of the request header, from 1 to 65535. • Response—The desired maximum length, in bytes, of the response header, from 1 to 65535. • Excessive Header Length Action—The action to take when the length is exceeded: – Allow Packet—Allow the message. – Drop Packet—Close the connection. – Reset Connection—Send a TCP reset message to client and server. • Generate Syslog—Whether to generate a syslog message when a violation occurs.

Table 17-32 HTTP Map Entity Length Tab (continued)

Element	Description
Inspect Body Length	Whether to enable inspection based on the length of the message body. If you select this option, configure the following: • Minimum Threshold—The desired minimum length, in bytes, of the message body, from 1 to 65535. • Maximum Threshold—The desired maximum length, in bytes, of the message body, from 1 to 65535. • Body Length Threshold Action—The action to take when the message body falls outside of the configured boundaries: – Allow Packet—Allow the message. – Drop Packet—Close the connection. – Reset Connection—Send a TCP reset message to client and server. • Generate Syslog—Whether to generate a syslog message when a violation occurs.

HTTP Map RFC Request Method Tab

Use the RFC Request Method tab to define the action to take when specific request methods are used in the HTTP request.

Navigation Path

Click the RFC Request Method tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-33 HTTP Map RFC Request Method

Element	Description
Available and Selected Methods	The Available Methods list contains the request methods defined in RFC 2616.
Action Generate Syslog	To configure an action for a method, select it, then select an action and optionally select **Generate Syslog** if you want a message added to the syslog when an HTTP request containing the selected method is encountered. Click the **>>** button to add it to the Selected Methods list. (To remove a method from the selected list, select it and click the **<<** button.) **Tip** You can select multiple methods at a time using Ctrl+click if the action and syslog requests are the same for each. The actions you can specify are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server.
Specify the action to be applied for the remaining available methods above.	Whether to define a default action for the methods for which you have not configured specific actions above. If you select this option, select the action and syslog setting to use for the default action.

HTTP Map Extension Request Method Tab

Use the Extension Request Method tab to define the action taken when specific extension request methods are used in the HTTP request.

Navigation Path

Click the Extension Request Method tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-34 HTTP Map Extension Request Method Tab

Element	Description
Available and Selected Methods	The Available Methods list contains the extension request methods defined in RFC 2616.
Action Generate Syslog	To configure an action for a method, select it, then select an action and optionally select **Generate Syslog** if you want a message added to the syslog when an HTTP request containing the selected method is encountered. Click the >> button to add it to the Selected Methods list. (To remove a method from the selected list, select it and click the << button.) **Tip** You can select multiple methods at a time using Ctrl+click if the action and syslog requests are the same for each. The actions you can specify are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server.
Specify the action to be applied for the remaining available methods above.	Whether to define a default action for the methods for which you have not configured specific actions above. If you select this option, select the action and syslog setting to use for the default action.

HTTP Map Port Misuse Tab

Use the Port Misuse tab to enable port misuse application firewall inspection. The application categories you can configure are:

- IM—Instant Messaging. The applications checked for are Yahoo! Messenger, AIM, and MSN IM.
- P2P—Peer-to-peer applications. The Kazaa application is checked.
- Tunneling—Tunneling applications. The applications checked for are HTTPort/HTTHost, GNU Httptunnel, GotoMyPC, Firethru, and Http-tunnel.com Client.

Navigation Path

Click the Port Misuse tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-35 HTTP Map Port Misuse Tab

Element	Description
Available and Selected Application Categories Action Generate Syslog	The Available Application Categories list contains the categories for which you can define firewall inspection settings. To configure an action for a category, select it, then select an action and optionally select **Generate Syslog** if you want a message added to the syslog when an HTTP request containing the selected application is encountered. Click the >> button to add it to the Selected Categories list. (To remove a category from the selected list, select it and click the << button.) **Tip** You can select multiple categories at a time using Ctrl+click if the action and syslog requests are the same for each. The actions you can specify are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server.
Specify the action to be applied for the remaining available categories above.	Whether to define a default action for the categories for which you have not configured specific actions above. If you select this option, select the action and syslog setting to use for the default action.

HTTP Map Transfer Encoding Tab

Use the Transfer Encoding tab to enable inspection based on the transfer encoding type. The encoding types that you can configure are:

- Chunked—Identifies the transfer encoding type in which the message body is transferred as a series of chunks.
- Compressed—Identifies the transfer encoding type in which the message body is transferred using UNIX file compression.
- Deflate—Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951).
- GZIP—Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952).
- Identity—Identifies connections in which no transfer encoding is performed in the message body.

Navigation Path

Click the Transfer Encoding tab on the Add and Edit HTTP Map dialog boxes for ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS Devices. See Configuring HTTP Maps for ASA 7.1.x, PIX 7.1.x, FWSM 3.x and IOS Devices, page 17-56.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-36 HTTP Map Transfer Encoding Tab

Element	Description
Available and Selected Encoding Types	The Available Encoding Types list contains the types of transfer encoding for which you can define firewall inspection settings.
Action Generate Syslog	To configure an action for a type, select it, then select an action and optionally select **Generate Syslog** if you want a message added to the syslog when an HTTP request containing the selected type is encountered. Click the **>>** button to add it to the Selected Encoding Types list. (To remove a type from the selected list, select it and click the **<<** button.) **Tip** You can select multiple types at a time using Ctrl+click if the action and syslog requests are the same for each. The actions you can specify are: • Allow Packet—Allow the message. • Drop Packet—Close the connection. • Reset Connection (default)—Send a TCP reset message to client and server.
Specify the action to be applied for the remaining available encoding types above.	Whether to define a default action for the types for which you have not configured specific actions above. If you select this option, select the action and syslog setting to use for the default action.

Configuring HTTP Maps for ASA 7.2+ and PIX 7.2+ Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX features/functionality, it does not support any enhancements.

Use the Add and Edit HTTP Map dialog boxes to define the match criterion and values for the HTTP inspect map for ASA and PIX software releases 7.2 and higher.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > HTTP (ASA 7.2+/PIX 7.2+)** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-37 Add and Edit HTTP Map Dialog Boxes (ASA 7.2+/PIX 7.2+)

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Body Match Maximum	The maximum number of characters in the body of an HTTP message that should be searched in a body match. **Tip** A high value can have a significant impact on performance.
Check for protocol violations	Whether to check for protocol violations.
Action	The action to take based on the defined settings. You can drop, reset, or log the connection.
Spoof Server	Enables you to replace the server HTTP header value with the specified string.

Match Condition and Action Tab

The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions.

- To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see HTTP Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-66).
- To edit a criterion, select it and click the Edit button.
- To delete a criterion, select it and click the Delete button.

Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.
Overrides: None	Shows that no overrides exist on the device. You must manually set overrides in order to change the display. For more information, see Understanding Policy Object Overrides for Individual Devices, page 6-18. **Note** Selecting Allow Value Override per Device does not automatically set overrides.

HTTP Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes

Note From version 4.17, though Cisco Security Manager continues to support PIX features/functionality, it does not support any enhancements.

Use the Add or Edit HTTP Match Criterion (for HTTP class maps) or Match Condition and Action (for HTTP policy maps) dialog boxes to do the following:

- Define the match criterion and value for an HTTP class map.
- Select an HTTP class map when creating an HTTP policy map.
- Define the match criterion, value, and action directly in an HTTP policy map.

These types of maps are used only for devices running ASA 7.2 or higher, or PIX 7.2 or higher, operating systems.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map. You can use the following criteria:

- Request/Response Content Type Mismatch—Specifies that the content type in the response must match one of the MIME types in the accept field of the request.
- Request Arguments—Applies the regular expression match to the arguments of the request.
- Request Body—Applies the regular expression match to the body of the request.
- Request Body Length—Specifies that the body length of the request be matched as greater than or less than the specified number of bytes.
- Request Header Count—Specifies that the number of headers in the request be matched as greater than or less than the specified number.
- Request Header Length—Specifies that the header length of the request be matched as greater than or less than the specified number of bytes.
- Request Header Field—Applies the regular expression match to the header of the request.
- Request Header Field Count—Applies the regular expression match to the header of the request based on a specified number of header fields.
- Request Header Field Length—Applies the regular expression match to the header of the request based on a specified field length.
- Request Header Content Type—Specifies the content type to evaluate in the content-type header field of the request.
- Request Header Transfer Encoding—Specifies the transfer encoding to evaluate in the transfer-encoding header field of the request.
- Request Header Non-ASCII—Specifies whether there are non-ASCII characters in the header of the request.
- Request Method—Specifies the method of the request to match.
- Request URI—Applies the regular expression match to the URI of the request.
- Request URI Length—Specifies that the URI length of the request be matched as greater than or less than the specified number of bytes.
- Response Body ActiveX—Specifies whether there is ActiveX content in the body of the request.
- Response Body Java Applet—Specifies whether there is a Java applet in the body of the request.

- Response Body—Applies the regular expression match to the body of the response.
- Response Body Length—Specifies that the body length of the response be matched as greater than or less than the specified number of bytes.
- Response Header Count—Specifies that the number of headers in the response be matched as greater than or less than the specified number.
- Response Header Length—Specifies that the header length of the response be matched as greater than or less than the specified number of bytes.
- Response Header Field—Applies the regular expression match to the header of the response.
- Response Header Field Count—Applies the regular expression match to the header of the response based on a specified number of header fields.
- Response Header Field Length—Applies the regular expression match to the header of the response based on a specified field length.
- Response Header Content Type—Specifies the content type to evaluate in the content-type header field of the response.
- Response Header Transfer Encoding—Specifies the transfer encoding to evaluate in the transfer-encoding header field of the response.
- Response Header Non-ASCII—Specifies whether there are non-ASCII characters in the header of the response.
- Response Status Line—Applies the regular expression match to the status line of the response.

Navigation Path

When creating an HTTP class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for HTTP, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating an HTTP policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit HTTP Map dialog boxes for ASA/PIX 7.2+ devices, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring HTTP Maps for ASA 7.2+ and PIX 7.2+ Devices, page 17-64.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-38 HTTP Class and Policy Maps (ASA 7.2+/PIX 7.2+) Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing HTTP class map or define a new HTTP class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing HTTP class map policy object. Enter the name of the HTTP class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of HTTP traffic to match. The criteria are described above.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. For some criteria, this is the only available option. • Doesn't Match—Does not match the criterion.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria. The types of action depend on the criterion you select.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Field Name	The name of the header field to evaluate. You can select one of the following: • Predefined—The predefined HTTP header fields. • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object.

Table 17-38 HTTP Class and Policy Maps (ASA 7.2+/PIX 7.2+) Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object. When you are evaluating the Request Header Transfer Encoding or Response Header Transfer Encoding criteria, you can also select these options: • Specified By—One of the following predefined types of transfer encoding: – Chunked—The message body is transferred as a series of chunks. – Compressed—The message body is transferred using UNIX file compression. – Deflate—The message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951). – GZIP—The message body is transferred using GNU zip (RFC 1952). – Identity—No transfer encoding is performed. • Empty—The transfer-encoding field in request header is empty.
Greater Than Length	The length in bytes of the evaluated field. The criterion matches if the length is greater than the specified number, and does not match if the field is less than the specified number.
Greater Than Count	The number of evaluated items. The criterion matches if the count is greater than the specified number, and does not match if the count is less than the specified number.

Table 17-38 HTTP Class and Policy Maps (ASA 7.2+/PIX 7.2+) Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Content Type	The content type to evaluate as specified in the content-type header field. You can select one of the following: • Specified By—A predefined MIME type. • Unknown—The MIME type is not known. Select Unknown when you want to evaluate the item against all known MIME types. • Violation—The magic number in the body must correspond to the MIME type in the content-type header field. • Regular Expression, Regular Expression Group—The regular expression or regular expression group to evaluate. See the explanation for the Value field for an explanation of these options.
Request Method	The specified request method to match. You can select one of the following: • Specified By—The predefined request method. • Regular Expression, Regular Expression Group—The regular expression or regular expression group to evaluate. See the explanation for the Value field for an explanation of these options.

Configuring IM Maps for ASA 7.2+, PIX 7.2+ Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX features/functionality, it does not support any enhancements.

Use the Add and Edit IM Map dialog boxes to define settings for define an Instant Messenger (IM) inspect map for devices running ASA/PIX 7.2 or higher. An IM map lets you change the default configuration values used for IM application inspection.

Instant Messaging causes concern due to its use of clear text when conducting business and the potential for network attacks and the spreading of viruses. Thus, you might want to block certain types of instant messages from occurring, while allowing others.

For ASA and PIX devices, IM application inspection provides detailed access control to control network usage. You can use regular expressions to help stop leakage of confidential data and the propagation of network threats. You can inspect Yahoo! Messenger or MSN Messenger traffic.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > IM (ASA 7.2+/PIX 7.2+)** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-39 Add and Edit IM Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Match Condition and Action Tab The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes, page 17-71). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes

Note From version 4.17, though Cisco Security Manager continues to support PIX features/functionality, it does not support any enhancements.

Use the Add or Edit IM Match Criterion (for IM class maps) or Match Condition and Action (for IM policy maps) dialog boxes to do the following:

- Define the match criterion and value for an IM class map.
- Select an IM class map when creating an IM policy map.
- Define the match criterion, value, and action directly in an IM policy map.

These types of maps are used only for devices running ASA 7.2 or higher, or PIX 7.2 or higher, operating systems.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating an IM class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for IM, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating an IM policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit IM Map dialog boxes for ASA 7.2/PIX 7.2, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring IM Maps for ASA 7.2+, PIX 7.2+ Devices, page 17-70.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-40 IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing IM class map or define a new IM class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing IM class map policy object. Enter the name of the IM class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of IM traffic to match. The criteria are: • Filename—Matches the filename from IM file transfer service. • Client IP Address—Matches the source client IP address. • Client Login Name—Matches the client login name from IM service. • Peer IP Address—Matches the peer, or destination, IP address. • Peer Login Name—Matches the peer, or destination, login name from IM service. • Protocol—Matches IM protocols. • Service—Matches IM services. • File Transfer Service Version—Matches the IM file transfer service version.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.

Table 17-40 IM Class and Policy Map (ASA 7.2+/PIX 7.2+) Add or Edit Match Condition (and Action) Dialog Boxes (continued)

Element	Description
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
IP Address	The IP address you want to match.
Protocol	The IM protocol, either MSN Messenger or Yahoo! Messenger.
Services	The IM services you want to inspect. Select one or more of the listed services.

Configuring IM Maps for IOS Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX, FWSM, and IPS features/functionality, it does not support any enhancements.

Use the Add and Edit IM Map (IOS) dialog boxes to configure Instant Messaging (IM) inspection policy map objects for IOS devices. An IM map lets you change the default configuration values used for IM application inspection.

Instant Messaging causes concern due to its use of clear text when conducting business and the potential for network attacks and the spreading of viruses. Thus, you might want to block certain types of instant messages from occurring, while allowing others.

IM application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and the propagation of network threats. The scope can be limited by identifying permitted or denied servers. Inspection of Yahoo! Messenger, MSN Messenger, and AOL instant messages are supported.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > IM (IOS)** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-41 Add and Edit IM Map (IOS) Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Service Tabs The tabs represent different IM service providers. The settings available on each tab are identical. You must configure the settings separately for each service provider. The descriptions of the following fields apply to each of the services: Yahoo!, MSN, and AOL.	
Text Chat	How you want the text chat service to be handled, for example, allowed, denied, logged, or some combination.
Other Services	How you want services other than text chat to be handled, for example, allowed, denied, logged, or some combination. IOS software recognizes all services other than text chat, such as voice-chat, video-chat, file sharing and transferring, and gaming as a single group.
Permit Servers	The servers from which to permit traffic. Accepted formats are IP addresses, IP ranges, and hostnames separated by commas.
Deny Servers	The servers from which to deny traffic. Accepted formats are IP addresses, IP ranges, and hostnames separated by commas.
Alert	Whether you want to enable or disable alerts. The default is to use the default inspection settings.
Audit	Whether you want to enable or disable an audit trail. The default is to use the default inspection settings.
Timeout	A timeout for the service. You can use the default inspection settings, or you can elect to specify a timeout. If you select Specify Timeout, enter the timeout value in seconds.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring IP Options Maps

Use the Add and Edit IP Options Map dialog boxes to define maps for the inspection of the options in an IP packet header on ASA 8.2(2)+ devices. The options field provides for control functions that are required in some situations but unnecessary for most common communications.

If you do not configure IP options inspection, the ASA device drops packets that have any options configured, with one exception. In routed mode, packets that contain the router alert option are allowed. (To disallow router alert packets, create an IP options map with router alert deselected, and configure an inspection rule to inspect IP Options using the policy map.)

Tip Because the no operation (NOP) option might be used as padding to ensure proper packet-header size and alignment, you might want to allow NOP.

For each option, you can select whether to:

- **Allow**—Allow the packet and do not change the IP header options field.
- **Clear**—Allow the packet and clear the option from the IP header options field.

If you do not select an option, the option is prohibited, and packets containing the option are dropped. Any option not listed here also results in a dropped packet; you cannot change this behavior.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > IP Options** from the Object Type selector. Right-click inside the work area, then select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-42 Add and Edit IP Options Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object.
End of Options List	End of Options List (EOOL), or IP Option 0, contains just a single zero byte and 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	No Operation (NOP), or IP Option 1, is used for padding. 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 to align the options on a 32-bit boundary.

Table 17-42 Add and Edit IP Options Map Dialog Boxes (continued)

Element	Description
Router alert	Router Alert (RTRALT), or IP Option 20, 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 require relatively complex processing from the routers along the packet's delivery path.
Basic Security *(ASA devices 9.5(1) or higher)*	IP-option Basic Security (number 130) from RFC 1108, default is to drop.
Commercial Security *(ASA devices 9.5(1) or higher)*	IP-option Commercial Security (number 134), default is to drop.
Default *(ASA devices 9.5(1) or higher)*	IP-option default configuration, default is drop.
Experimental Flow Control *(ASA devices 9.5(1) or higher)*	IP-option Experimental Flow Control (number 205), default is to drop.
Experimental Measurement *(ASA devices 9.5(1) or higher)*	IP-option Experimental Measurement (number 10), default is to drop.
Extended-Security *(ASA devices 9.5(1) or higher)*	IP-option Extended Security (number 133) from RFC 1108, default is to drop.
IMI Traffic Descriptor *(ASA devices 9.5(1) or higher)*	IP-option IMI Traffic Descriptor (number 144), default is to drop.
Quick Start *(ASA devices 9.5(1) or higher)*	IP-option Router Alert (number 25) from RFC 4782, default is to drop.
Record Route *(ASA devices 9.5(1) or higher)*	IP-option Record Route (number 7) from RFC 791, default is to drop.
Time Stamp *(ASA devices 9.5(1) or higher)*	IP-option Router Alert (number 68) from RFC 791, default is to drop.
Note Beginning with version 4.9, Security Manager supports 10 new IP Options for ASA devices running the software version 9.5(1) or higher. You can tune the inspection to allow, clear, or drop any standard or experimental options. You can also configure specific IP Options apart from the ones that are defined. For example, a value ranging between 0 and 255 can be used to configure an IP Option directly. Security Manager supports the CLI '[no] 0-255 allow | clear'. You can also set a default behavior for options not explicitly defined in an IP options inspection map. You now select which options to allow and optionally clear. 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	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 17-42 Add and Edit IP Options Map Dialog Boxes (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring IPv6 Maps

Use the Add and Edit IPv6 Map dialog boxes to define the match criteria and values for an IPv6 inspect map. You can use an IPv6 map to selectively drop IPv6 packets based on following types of extension headers found anywhere in the IPv6 packet:

- Hop-by-Hop Options
- Routing (Type 0)
- Fragment
- Destination Options
- Authentication
- Encapsulating Security Payload

Service objects corresponding to these protocols are available in the Services table in the Policy Object Manager, page 6-4.

Note With the release of Security Manager 4.4 and versions 9.0 and higher of the ASA, the separate policies for configuring IPv4 and IPv6 inspection rules were unified. However, IPv6 maps are still provided in support of earlier versions.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > IPv6** from the Object Type selector. Right-click inside the table, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-43 Add and Edit IPv6 Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.

Table 17-43 Add and Edit IPv6 Map Dialog Boxes (continued)

Element	Description
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Permit only known Extension Headers	Whether the ASA should verify the IPv6 extension header. When selected and an unknown IPv6 extension header is encountered, the ASA drops the packet and logs the action. This option is selected by default.
Enforce Extension Header Order	Whether the ASA should enforce extension header order as defined in the RFC 2460 specification. When selected and an error is detected, the ASA drops the packet and logs the action. This option is selected by default.

Match Condition and Action Tab

The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions.

These criteria entries are created and edited in the IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-78.

Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides in the Policy Object Overrides Window, page 6-20. The **Overrides** field indicates the number of devices that have overrides for this object.

IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Add or Edit Match Condition and Action dialog boxes to define an Extension Header match criterion and action for an IPv6 policy map. The contents of the Extension Headers are not processed; an action is applied based solely on the presence of a specified EH type.

The fields in these dialog boxes change based on the criterion you select.

Note You can apply multiple match definitions to one IPv6 policy map.

Navigation Path

In the Policy Object Manager, from the Match Condition and Action tab on the Add or Edit IPv6 Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring IPv6 Maps, page 17-77.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-44 IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Choose the type of IPv6 Extension Header to match: • Authentication Header (AH)—Provides integrity and data-origin authentication for IP packets. • Destination Options Header—Used for IPv6 Mobility, as well as in support of certain applications. • Encapsulating Security Payload Header (ESP)—All information following the ESP header is encrypted and not accessible to intermediate network devices. • Fragment Header—Supports traffic-source fragmented-packet communications. • Hop-by-Hop Options Header—Optional information that must be examined by every node in the packet's delivery path. • Header Count—The number of headers in the packet. When you choose this option, the following field appears; specify an upper bound for the number of headers: – Greater Than Count—Enter a value between 0 and 255. The packet is considered a match if the Header Count is greater than the specified number; it is not a match if the count is equal to, or less than the specified number. • Routing Header Type—Use this option to match one or EH types based on their header codes. When you choose this type, the following Value options appear; specify one or the other: – Routing Type—Enter one Extension Header code; for example, *51* for Authentication Header. – Routing Type Field Range—Enter a starting value and an ending value to define a range of EH codes. • Routing Header Address Count—The number of IP addresses embedded in the packet. When you choose this option, the following field appears; specify an upper bound for the number of addresses: – Greater Than Count—Enter a value between 0 and 255. The packet is considered a match if the address count is greater than the specified number; it is not a match if the count is equal to, or less than the specified number.
Type	Specifies that the map is applied only to traffic that matches the defined criteria.

Table 17-44 IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Action	Choose the action you want the device to take for traffic that matches the defined criteria: • Drop Packet—Matching packets are dropped without notification. • Drop Packet and Log—Matching packets are logged and then dropped. • Log—Matching packets are logged and processing continues.

Configuring IPsec Pass Through Maps

Use the Add and Edit IPsec Pass Through Map dialog boxes to configure settings for the IPsec Pass Through Map policy object. An IPsec Pass Through policy map lets you change the default configuration values used for IPsec Pass Through inspection.

The IPSec Pass Through inspection engine lets the security appliance pass ESP (IP protocol 50) and AH (IP protocol 51) traffic that is formed between two hosts because of successful IKE (UDP port 500) negotiation without the requirement of specific ESP or AH access lists.

The ESP or AH traffic is permitted by the inspection engine with the configured idle timeout if there is an existing control flow and it is within the connection limit defined in the MPF framework. A new control flow is created for IKE UDP port 500 traffic with the configured UDP idle timeout if there is not one, or it uses the existing flow.

To ensure that the packet arrives into the inspection engine, a hole is punched for all such traffic (ESP and AH). This inspect is attached to the control flow. The control flow is present as long as there is at least one data flow (ESP or AH) established, but the traffic always flows on the same connection. Because this IKE connection is kept open as long as data flows, a rekey would always succeed. The flows are created irrespective of whether NAT is being used. However, PAT is not supported.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > IPsec Pass Through** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-45 Add and Edit IPsec Pass Through Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.

Table 17-45 Add and Edit IPsec Pass Through Map Dialog Boxes (continued)

Element	Description
Allow ESP Maximum ESP Tunnels per Client ESP Idle Timeout	Whether to allow ESP traffic. If you select this option, you can configure the maximum number of ESP tunnels that each client can have and the amount of time that an ESP tunnel can be idle before it is closed (in hours:minutes:seconds format). The default timeout is 10 minutes (00:10:00).
Allow AH Maximum AH Tunnels per Client AH Idle Timeout	Whether to allow AH traffic. If you select this option, you can configure the maximum number of AH tunnels that each client can have and the amount of time that an AH tunnel can be idle before it is closed (in hours:minutes:seconds format). The default timeout is 10 minutes (00:10:00).
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring NetBIOS Maps

Use the Add or Edit NetBIOS Map dialog boxes to define maps for NetBIOS inspection. A NetBIOS policy map lets you change the default configuration values used for NetBIOS inspection.

The NetBIOS inspection engine translates IP addresses in the NetBIOS name service (NBNS) packets according to the security appliance NAT configuration.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > NetBIOS** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-46 Add or Edit NetBIOS Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.

Table 17-46 Add or Edit NetBIOS Map Dialog Boxes (continued)

Element	Description
Check for Protocol Violation Action	Whether to check for NETBIOS protocol violations. If you select this option, select the action you want to take when violations occur.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring ScanSafe Maps

Use the Add or Edit ScanSafe Map dialog boxes to define maps for ScanSafe inspection. A ScanSafe policy map lets you change the default configuration values used for ScanSafe inspection.

The fields on this dialog box change, depending upon whether you are creating a class map or a policy map.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > ScanSafe** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-47 ScanSafe Add Match Condition and Action Dialog Box

Element	Description
Parameters	
Transport Protocol	Allows you to select either HTTPS or HTTP. For HTTPS, the allowed range of values is 1-65535. For HTTP, the allowed range of values is 1-65535. The default value is 8080.
Default User Name	The default user name for the ScanSafe server
Default Group Name	The default group name for the ScanSafe server

Table 17-47 ScanSafe Add Match Condition and Action Dialog Box (continued)

Element	Description
Parameters	
Category	Allows you to select Cat-A through Cat-G. This is the category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.
Match Condition and Action tab only	
Class	The name of the class map
Action	Allows you to select the action you want to take when policy violations occur
+ [the "add" button]	Opens the Add Match Condition and Action dialog box. This dialog box has the following fields: • Match Type • Class Map • Action

Configuring SIP Maps

Use the Add and Edit SIP Map dialog boxes to configure values used for SIP application inspection. A SIP inspection map lets you change the default configuration values used for SIP application inspection.

SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.

SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks. It also supports application security and protocol conformance, which enforce the sanity of the SIP messages, as well as detect SIP-based attacks.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > SIP (ASA/PIX/FWSM)** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-48 Add and Edit SIP Map Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Enable SIP Instant Messaging Extensions	Whether to enable Instant Messaging extensions.
Permit Non-SIP Traffic on SIP Port	Whether to permit non-SIP traffic on the SIP port.
Hide Server's and Endpoint's IP Address	Whether to hide the IP addresses, which enables IP address privacy.
Check RTP Packets for Protocol Conformance Limit Payload to Audio or Video based on the Signaling Exchange	Whether to check RTP/RTCP packets flowing on the pinholes for protocol conformance. If you select this option, you can also elect to enforce the payload type to be audio/video based on the signaling exchange.
If Number of Hops to Destination is Greater Than 0	Whether to check if the value of Max-Forwards header is zero. When it is greater than zero, the action you select in the Action field is implemented. The default is to drop the packet.
If State Transition is Detected	Whether to check SIP state transitions. When a transition is detected, the action you select in the Action field is implemented. The default is to drop the packet.
If Header Fields Fail Strict Validation	Whether to take the action specified in the Action field if the SIP header fields are invalid. The default is to drop the packet.
Inspect Server's and Endpoint's Software Version	Whether to inspect the SIP endpoint software version in User-Agent and Server headers. The default is to mask the information.
If Non-SIP URI is Detected	Whether to take the action specified in the Action field if a non-SIP URI is detected in the Alert-Info and Call-Info headers. The default is to mask the information.
Match Condition and Action Tab The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see SIP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-85). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 17-48 Add and Edit SIP Map Dialog Box (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

SIP Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit SIP Match Criterion (for SIP class maps) or Match Condition and Action (for SIP policy maps) dialog boxes to do the following:

- Define the match criterion and value for a SIP class map.
- Select a SIP class map when creating a SIP policy map.
- Define the match criterion, value, and action directly in a SIP policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating a SIP class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for SIP, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating a SIP policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit SIP Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring SIP Maps, page 17-83.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-49 SIP Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type Class Name (Policy Map only)	Enables you to use an existing SIP class map or define a new SIP class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing SIP class map policy object. Enter the name of the SIP class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.

Table 17-49 SIP Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Specifies which criterion of SIP traffic to match. • Called Party—Matches the called party as specified in the To header. • Calling Party—Matches the calling party as specified in the From header. • Content Length—Matches the Content Length header. • Content Type—Matches the Content Type header. • IM Subscriber—Matches the SIP Instant Messenger subscriber. • Message Path—Matches the SIP Via header. • Third Party Registration—Matches the requester of a third-party registration. • URI Length—Matches a URI in the SIP headers. • Request Method—Matches the SIP request method.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
Value	The regular expression you want to evaluate. You can select one of the following: • Regular Expression—The regular expression object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression object. • Regular Expression Group—The regular expression group object that defines the regular expression you want to use for pattern matching. Enter the name of the object. You can click **Select** to choose the object from a list of existing ones or to create a new regular expression group object.
URI Type	The type of URI to match, either SIP or TEL.
Greater Than Length	The length in bytes of the evaluated field. The criterion matches if the length is greater than the specified number, and does not match if the field is less than the specified number.

Table 17-49 SIP Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Content Type	The content type to evaluate as specified in the content-type header field. You can select one of the following: • SDP—Matches an SDP SIP content header type. • Regular Expression, Regular Expression Group—The regular expression or regular expression group to evaluate. See the explanation for the Value field for an explanation of these options.
Resource Method	The request method you want to inspect: • ack—Confirms that the client has received a final response to an INVITE request. • bye—Terminates a call and can be sent by either the caller or the called party. • cancel—Cancels any pending searches but does not terminate a call that has already been accepted. • info—Communicates mid-session signaling information along the signaling path for the call. • invite—Indicates a user or service is being invited to participate in a call session. • message—Sends instant messages where each message is independent of any other message. • notify—Notifies a SIP node that an event which has been requested by an earlier SUBSCRIBE method has occurred. • options—Queries the capabilities of servers. • prack—Provisional response acknowledgment. • refer—Requests that the recipient REFER to a resource provided in the request. • register—Registers the address listed in the To header field with a SIP server. • subscribe—Requests notification of an event or set of events at a later time. • unknown—Uses a nonstandard extension that could have unknown security impacts on the network. • update—Permits a client to update parameters of a session but has no impact on the state of a dialog.

Configuring Skinny Maps

Use the Add or Edit Skinny Map dialog boxes to define Skinny maps for Skinny inspection. A Skinny policy map lets you change the default configuration values used for Skinny inspection.

Skinny (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323 compliant terminals. Application layer functions in the security appliance recognize SCCP version 3.3. There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2.

The security appliance supports all versions through 3.3.2. The security appliance supports PAT and NAT for SCCP. PAT is necessary if you have more IP phones than global IP addresses for the IP phones to use. By supporting NAT and PAT of SCCP Signaling packets, Skinny application inspection ensures that all SCCP signaling and media packets can traverse the security appliance.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The security appliance also supports DHCP options 150 and 66, which it accomplishes by sending the location of a TFTP server to Cisco IP Phones and other DHCP clients. Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > Skinny** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-50 Add and Edit Skinny Map Dialog Boxes

Element	Description
Name	The name of the Skinny map. A maximum of 40 characters is allowed.
Description	A description of the Skinny map, up to 200 characters.
Parameters Tab	
Enforce Endpoint Registration	Whether to enforce registration before calls can be placed.
Maximum SCCP Station Message ID 0x	The maximum SCCP station message ID allowed, in hexadecimal.
Check RTP Packets for Protocol Conformance Enforce Payload Type to be Audio or Video based on Signaling Exchange	Whether to check RTP packets flowing through the pinholes for protocol conformance. If you select this option, you can also select whether to enforce the payload type.
Minimum SCCP Prefix Length	The minimum SCCP length allowed.
Maximum SCCP Prefix Length	The maximum SCCP length allowed.
Media Timeout	The timeout value for media connections.
Signaling Timeout	The timeout value for signaling connections.

Table 17-50 Add and Edit Skinny Map Dialog Boxes (continued)

Element	Description
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see Skinny Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-89). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Skinny Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Add or Edit Match Condition and Action dialog boxes to define the match criterion, value, and action for a Skinny policy map.

Navigation Path

In the Policy Object Manager, from the Match Condition and Action tab on the Add or Edit Skinny Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring SIP Maps, page 17-83.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-51 Skinny Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Specifies which criterion of Skinny traffic to match.
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on 0xFFFF, then any traffic that has the message ID 0xFFFF is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.

Table 17-51 Skinny Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
ID Type	The hexadecimal value for the message ID to inspect: • Value—Matches a single hexadecimal value. • Range—Matches a range of values.
Action	The action you want the device to take for traffic that matches the defined criteria.

Configuring SNMP Maps

Use the Add and Edit SNMP Map dialog boxes to define maps for SNMP inspection. An SNMP policy map lets you change the default configuration values used for SNMP application inspection.

SNMP application inspection lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The security appliance can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map. You then apply the SNMP map when you enable SNMP inspection.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > SNMP** from the Object Type selector. Right-click inside the work area, then select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-52 Add and Edit SNMP Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Disallowed SNMP Versions	The versions of SNMP you want to prohibit. • SNMP Version 1 • SNMP Version 2c (Community Based) • SNMP Version 2 (Party Based) • SNMP Version 3
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 17-52 Add and Edit SNMP Map Dialog Boxes (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring SCTP Maps

SCTP is a transport-layer protocol operating on top of IP in the protocol stack, similar to TCP and UDP. SCTP creates a logical communication channel, called an association, between two end nodes over multiple source or destination IP addresses. An association defines a set of IP addresses on each node (source and destination) and a port on each node. Any IP address can be used as either a source or a destination IP address of data packets in the association. Messages can be transmitted between a pair of IP addresses, which is defined as a stream.

If you have SCTP traffic going through the ASA, you can configure Cisco Security Manager to control access based on SCTP ports, and implement application layer inspection to enable connections and to optionally filter on payload protocol ID (PPID) to selectively drop, log, or rate limit applications.

You can refine your access rules by adding an SCTP inspect map and filtering on SCTP applications.You can selectively drop, log, or rate limit SCTP traffic classes based on the payload protocol identifier (PPID).

When you filter on PPID, keep the following in mind:

- PPIDs are in data chunks, and a given packet can have multiple data chunks. If a packet includes data chunks with different PPIDs, the packet will not be filtered, and the assigned action will not be applied to the packet.
- If you use PPID filtering to drop or rate-limit packets, be aware that the transmitter will resend any dropped packets. Although a packet for a rate-limited PPID might make it through on the next attempt, a packet for a dropped PPID will again be dropped. You might want to evaluate the eventual consequence of these repeated drops on your network.

Use the Add and Edit SCTP Map dialog boxes to define the match criteria and values for an SCTP inspect map. You can use an SCTP map to inspect packets based on the Payload PID criteria. You can perform the following actions on the packets, based on the PPID match criteria:

- No Action
- Drop Packet
- Log Packet
- Rate Limit

Service objects corresponding to the SCTP protocol are available in the Services table in the Policy Object Manager, page 6-4.

Note SCTP inspect maps are supported from Security Manager 4.10 and ASA versions 9.5.2 and higher.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > SCTP** from the Object Type selector. Right-click inside the table, then select **New Object** or right-click a row, then select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-53 Add and Edit SCTP Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. These criteria entries are created and edited in the SCTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-92.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides in the Policy Object Overrides Window, page 6-20. The **Overrides** field indicates the number of devices that have overrides for this object.

SCTP Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Add or Edit Match Condition and Action dialog boxes to define a Payload PID match criterion and action for a SCTP policy map. Repeat the process until you identify all PPIDs you want to selectively handle.

Navigation Path

In the Policy Object Manager, from the Match Condition and Action tab on the Add or Edit IPv6 Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring IPv6 Maps, page 17-77.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-54 IPv6 Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Select the Payload PID (PPID) criterion.
Type	Specifies that the map is applied only to traffic that matches or does not match the defined criteria.
You can find the current list of SCTP PPIDs at http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25.	
Min. Payload PID	Enter a PPID number. There are certain PPIDs associated with a name, which Cisco Security Manager accepts, and processes internally. Enter the PPID number in the text box, and click OK. The corresponding name will be displayed in the match action table if it matches the default names.
Max. Payload PID	(Optional) Enter a second, higher PPID to specify a range of PPIDs.
Action	Choose the action based on the PPID in SCTP data chunks: • Drop Packet—Drop and log all packets that match. • Log—Send a system log message. • Rate Limit— Limit the rate of messages. The rate is in packets per second.

Configuring Diameter Maps

Diameter is an Authentication, Authorization, and Accounting (AAA) protocol used in next-generation mobile and fixed telecom networks such as EPS (Evolved Packet System) for LTE (Long Term Evolution) and IMS (IP Multimedia Subsystem). It replaces RADIUS and TACACS in these networks.

Diameter uses TCP and SCTP as the transport layer, and secures communications using TCP/TLS and SCTP/DTLS. It can optionally provide data object encryption as well. For detailed information on Diameter, see RFC 6733.

Diameter applications perform service management tasks such as deciding user access, service authorization, quality of service, and rate of charging. Although Diameter applications can appear on many different control-plane interfaces in the LTE architecture, the ASA inspects Diameter command codes and attribute-value pairs (AVP) for the following interfaces only:

- S6a: Mobility Management Entity (MME) - Home Subscription Service (HSS).
- S9: PDN Gateway (PDG) - 3GPP AAA Proxy/Server.
- Rx: Policy Charging Rules Function (PCRF) - Call Session Control Function (CSCF).

Diameter inspection opens pinholes for Diameter endpoints to allow communication. The inspection supports 3GPP version 12 and is RFC 6733 compliant.

You can use the Add and Edit Diameter Map dialog boxes to filter traffic based on application ID, command codes, and AVP, to apply special actions such as dropping packets or connections, or logging them. You can create custom AVP for newly-registered Diameter applications. Filtering lets you fine-tune the traffic you allow on your network. For more information see Create and Add Custom AVPs, page 17-97

Note Diameter messages for applications that run on other interfaces will be allowed and passed through by default. However, you can configure a Diameter inspection policy map to drop these applications by application ID, although you can specify actions based on the command codes or AVP for these unsupported applications.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > Diameter** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28
- Create and Add Custom AVPs, page 17-97

Field Reference

Table 17-55 Add and Edit Diameter Map Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Unsupported application-id action log	To log unsupported Diameter application identifier (Diameter application name) in the map. Application ID is a number between 0-4294967295, in the map. These applications are registered with the IANA. Following are the core supported applications, but you can filter on other applications. **3gpp-rx-ts29214** (16777236) **3gpp-s6a** (16777251) **3gpp-s9** (16777267) **common-message** (0) - This is the base Diameter protocol
Unsupported command code action log	To log unsupported Diameter command codes in the map, where *code* is the Diameter command code name or number (0-4294967295).
Unsupported avp action log	To log unsupported attribute- value pair parameter
Strict Parameters	
Enable Session Validation	To validate session-ID AVP related messages
Enable State Validation	To enable validation of state machine

Table 17-55 Add and Edit Diameter Map Dialog Box (continued)

Element	Description
Match Condition and Action Tab	
	The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see Diameter Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes, page 17-95). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Diameter Class and Policy Maps Add or Edit Match Condition (and Action) Dialog Boxes

Use the Add or Edit Diameter Match Criterion (for Diameter class maps) or Match Condition and Action (for Diameter policy maps) dialog boxes to do the following:

- Define the match criterion and value for a Diameter class map.
- Select a Diameter class map when creating a Diameter policy map.
- Define the match criterion, value, and action directly in a Diameter policy map.

The fields on this dialog box change based on the criterion you select and whether you are creating a class map or policy map.

Navigation Path

When creating a Diameter class map, in the Policy Object Manager, from the Add or Edit Class Maps dialog boxes for Diameter, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Class Maps for Inspection Policies, page 17-28.

When creating a Diameter policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit Diameter Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring Diameter Maps, page 17-93.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-56 Diameter Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Match Type (Only Policy Map)	Enables you to use an existing Diameter class map or define a new Diameter class map. • Use Specified Values—You want to define the class map on this dialog box. • Use Values in Class Map—You want to select an existing Diameter class map policy object. Enter the name of the Diameter class map in the **Class Name** field. Click **Select** to select the map from a list or to create a new class map object.
Criterion	Specifies which criterion of Diameter traffic to match. • Application ID—Matches the application identifier, where the application identifier is the Diameter application name or number (0-4294967295) in the **Begin Value** field. If there is a range of consecutively-numbered applications that you want to match, you can include a second ID in the **End Value** field. You can define the range by application name or number, and it applies to all the numbers between the **Begin Value** and the **End Value**. • Command Code—Matches the command code, where *code* is the Diameter command code name or number (0-4294967295) in the **Begin Value** field. If there is a range of consecutively-numbered command codes that you want to match, you can include a second code in the **End Value** field. You can define the range by command code name or number, and it applies to all the numbers between the **Begin Value** and the **End Value**. • AVP—Matches the Attribute Value Pair. – To match AVP based on attribute only, specify the name or number (1-4294967295) of an attribute-value pair. For the first code, you can specify the name of a custom AVP or one that is registered in RFCs or 3GPP technical specifications and is directly supported in the software in the **Begin Value** field. If you want to match a range of AVP, specify the second code by number only in the **End Value** field. If you want to match an AVP by its value, you cannot specify a second code. Specify the ID number of the vendor to also match, from 0-4294967295 in the **Vendor ID** field. For example, the 3GPP vendor ID is 10415, the IETF is 0. – To match AVP based on the value of the attribute, additionally specify the value of the attribute in the **AVP Data Type** field. **Note** You can create and add custom AVPs to new diameter applications. For more information see, Create and Add Custom AVPs, page 17-97

Table 17-56 Diameter Class and Policy Maps Add and Edit Match Condition and Action Dialog Boxes (continued)

Element	Description
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Variable Fields The following fields vary based on what you select in the Criterion field. This list is a super-set of the fields you might see.	
AVP DataType	You can configure this only if the data type of the AVP is supported. For example, you can specify an IP address for AVP that have the address data type. Following are the specific syntax of the value option for the supported data types • Address—Specify the IPv4 or IPv6 address to match. For example, 10.100.10.10 or 2001:DB8::0DB8:800:200C:417A • Diameter Identity, Diameter URI, Octet String, UTF8tString—Use regular expression or regular expression class objects to match these data types. • Enumerated—Specify a range of numbers in the Begin Range and End Range fields. The range is 0 - 4294967295. • Float32: decimal point representation with 8 digit precision • Float64: decimal point representation with 16 digit precision • Integer32: -2147483647 to 2147483647 • Integer64: -9223372036854775807 to 9223372036854775807 • Unsigned32: 0 to 4294967295 • Unsigned64: 0 to 18446744073709551615 • Time— Specify the start and end dates and time. Both are required. Time is in 24-hour format. **Note** You can create and add custom AVPs to new Diameter applications.
Action (Policy Map only)	The action you want the device to take for traffic that matches the defined criteria.

Create and Add Custom AVPs

Use the Add AVP dialog boxes to create and add custom AVPs. These can be registered with the IETF and added to new Diameter applications.

Note Cisco Security Manager does not allow you to edit a custom AVP object, once created.However the Device Override option allows you to edit the custom AVP for a particular device. If you want to change any parameter in the custom AVP object, you have to remove the custom AVP reference from the diameter building block (if it is referred), deploy to the device (if it is present in the device) and re-create the object with the required values and refer it back in the diameter building block and deploy it again.

Navigation Path

When creating a custom AVP, in the Policy Object Manager, from the Add Match Criterion dialog box for Diameter, select **AVP in the Criterion**, then select **Begin Value and right click in the AVP Maps Selector dialog box to Add AVP.**

Field Reference

Table 17-57 Add AVP Dialog Boxes

Element	Description
Name	The name of the custom AVP. A maximum of 32 characters is allowed. **Note** At least one character of the name must be an alphabet.
Description	A description of the AVP. A maximum of 80 characters is allowed.
AVP Code	Set a value for the AVP Code (256- 4294967295), that belongs to the specific vendor code address space.
DataType	You can configure this only if the data type of the AVP is supported. For example, you can specify an IP address for AVP that have the address data type. Following are the specific syntax of the value option for the supported data types • Address—Specify the IPv4 or IPv6 address to match. For example, 10.100.10.10 or 2001:DB8::0DB8:800:200C:417A • Diameter Identity, Diameter URI, Octet String, UTF8tString—Use regular expression or regular expression class objects to match these data types. • Enumerated—Specify a range of numbers in the Begin Range and End Range fields. The range is 0 - 4294967295. • Float32: decimal point representation with 8 digit precision • Float64: decimal point representation with 16 digit precision • Integer32: -2147483647 to 2147483647 • Integer64: -9223372036854775807 to 9223372036854775807 • Unsigned32: 0 to 4294967295 • Unsigned64: 0 to 18446744073709551615 • Time— Specify the start and end dates and time. Both are required. Time is in 24-hour format.
Vendor ID	Specify the ID number of the vendor, from 0-4294967295 in the **Vendor ID** field. For example, the 3GPP vendor ID is 10415, the IETF is 0.

Table 17-57 Add AVP Dialog Boxes (continued)

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Create and Add TLS Proxy Objects

If a Diameter application uses encrypted data over TCP, inspection cannot see inside the packets to implement your message filtering rules. Thus, if you create filtering rules, and you want them to also apply to encrypted TCP traffic, you must configure a TLS proxy. You also need a proxy if you want strict protocol enforcement on encrypted traffic. This configuration does not apply to SCTP/DTLS traffic.

The TLS proxy acts as a man-in-the-middle. It decrypts traffic, inspects it, then encrypts it again and sends it to the intended destination. Thus, both sides of the connection, the Diameter server and Diameter client, must trust the ASA, and all parties must have the required certificates. You must have a good understanding of digital certificates to implement TLS proxy.

Note The TLS proxy feature is supported in multi-context devices for version ASA 9.7.1 and higher.

You have the following options for configuring TLS proxy for Diameter inspection:

- Full TLS proxy—Encrypt traffic between the ASA and Diameter clients and the ASA and Diameter server. You have the following options for establishing the trust relationship with the server:
  - Use a static proxy client trustpoint. The ASA presents the same certificate for every Diameter client when communicating with the Diameter server. Because all clients look the same, the Diameter server cannot provide differential services per client. On the other hand, this option is faster than the LDC method.
  - Use local dynamic certificates (LDC). With this option, the ASA presents unique certificates per Diameter client when communicating with the Diameter server. This method gives the Diameter server better visibility into client traffic, which makes it possible to provide differential services based on client characteristics.
- TLS offload—Encrypt traffic between the ASA and Diameter client, but use a clear-text connection between the ASA and Diameter server. This option is viable if the Diameter server is in the same data center as the ASA, where you are certain that the traffic between the devices will not leave the protected area. Using TLS offload can improve performance, because it reduces the amount of encryption processing required. It should be the fastest of the options. The Diameter server can apply differential services based on client IP address only.

Navigation Path

Select **Manage > Policy Objects**, then select **TLS Proxy** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object.**

Field Reference

Table 17-58 Add TLS Proxy Dialog Boxes

Element	Description
Name	The name of the TLS Proxy object. A maximum of 63 characters is allowed. **Note** At least one character of the name must be an alphabet.
Description	A description of the TLS Proxy object.
Server Configuration	
Server Proxy Certificate	Click **Select** to import the CA certificate that is used to sign the Diameter client's certificate into an ASA trustpoint. This step specifies the proxy trustpoint certificate to be presented during TLS handshake. The trustpoint could be self-signed or issued by a third party. This allows the ASA to trust the Diameter clients.
Enable client authentication during TLS proxy handshake	Select to require the ASA to present a certificate and authenticate the TLS client during TLS handshake.
Encryption (Optional)	Beginning with 4.14, Cisco Security Manager allows you to configure cipher suites, when TLS Proxy is used as server. This field defines the cipher suites to be announced/matched during the TLS handshake. Select the Hashing algorithms, which are needed for encryption of data, from the Available Members List and add them to Selected Members list.
Client Configuration	
Configure the proxy client to use clear text to communicate with the remote TCP server	Select proxy client to use clear text, if encryption is not needed.
Specify the proxy certificate for the TLS client. The client proxy certificate could either be self-signed, enrolled with a CA or issued by a third party.	Select to specify Client Proxy Certificate. Alternately, click **Select** to import the CA certificate for the TLS client.
Specify the internal Certificate Authority to sign the local dynamic certificates for phones. This local CA can be self-signed certificate with proxy-ldc-issuer enabled or you may use embedded Local CA Server to issue LDC to phones.	Select to specify Local Dynamic Certificate Issuer. Alternately, click **Select** to import the CA certificate, which could serve as Local Dynamic certificate (LDC) issuer

Table 17-58 Add TLS Proxy Dialog Boxes (continued)

Element	Description
Local Dynamic Certificate Key Pair	
Key Pair Name	Specifies the RSA key pair to be used by the client or server's dynamic certificates. The key pair must have been generated with the "crypto key generate" command. The keypair must exist on the device before deployment.
Encryption (Optional)	Defines the cipher suites to be announced/matched during the TLS handshake. For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suites replace the original ones from the Hello message for asymmetric encryption method between the two TLS legs. Select the Hashing algorithms, which are needed for encryption of data, from the Available Members List and add them to Selected Members list. **Note** From ASA version 9.7.1, the Cisco Security Manager supports TLS1.2 new cipher suites— aes256-sha384 and aes128-sha256.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Editing TLS Proxy Object

Cisco Security Manager does not allow you to edit a TLS proxy object, once created. However, the Device Override option allows you to edit the TLS proxy object for a particular device.

If you want to change any parameter in the TLS proxy object, you have to remove the TLS proxy reference from the diameter building block (if it is referred), deploy to the device (if it is present in the device) and re-create the object with a new name, with the required values and refer it back in the diameter building block and deploy it again.

To edit a TLS proxy in class-map, execute the following deployment procedure:

1. Remove the relevant class map with existing TLS proxy server from the device by navigating to **Platform > Service Policy > Rules**.
2. Deploy the relevant class map with new TLS proxy server to the device by navigating to **Platform > Service Policy > Rules**.

Configuring LISP Maps

The Locator ID Separation Protocol (LISP) is a network architecture and protocol. LISP replaces a single IP address with two numbering spaces—Routing Locators (RLOCs), which are topologically assigned to network attachment points and used for routing and forwarding of packets through the network; and Endpoint Identifiers (EIDs), which are assigned independently from the network topology and used for numbering devices, and are aggregated along administrative boundaries.

LISP defines functions for mapping between the two numbering spaces and encapsulating traffic originated by devices using non-routable EIDs for transport across a network infrastructure that routes and forwards using RLOCs. LISP provides a set of functions for devices to exchange information that is used to map non-routable EIDs to routable RLOCs.

When considering the deployment of ACLs with LISP, the following aspects are important.

- LISP encapsulation utilizes a UDP header just prior to the LISP header for all packets to distinguish between two distinct packet groups: LISP control plane packets, which utilize a UDP destination port of 4342, and LISP data plane packets, which utilize a UDP destination port of 4341. ACLs may need to consider this distinction between these two groups of packets.
- LISP is an encapsulation protocol and, because ACLs only filter based on Layer 3 and Layer 4 header information, ACLs may need to be applied at a specific point or at several different points within the packet forwarding and LISP encapsulation process in order to implement a site security policy. The application point and direction of the ACL will dictate whether EID namespace or RLOC namespace is used within the ACL itself. Packets can be filtered using EID namespace just prior to LISP encapsulation or just after LISP decapsulation; packets can be filtered using RLOC namespace just after LISP encapsulation or just prior to LISP decapsulation.

You can use the Add and Edit LISP Map dialog boxes to filter traffic based on EID access-list and validation key. Filtering lets you fine-tune the traffic you allow on your network.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > LISP** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-59 Add and Edit LISP Map Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
Allowed Eid access-list	Enables you to select a unified access list building block.
Validation key	Specify an unencrypted clear text password.

Table 17-59 Add and Edit LISP Map Dialog Box (continued)

Element	Description
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring M3UA Maps

MTP3 User Adaptation (M3UA) is a client/server protocol that provides a gateway to the SS7 network for IP-based applications that interface with the SS7 Message Transfer Part 3 (MTP3) layer. M3UA makes it possible to run the SS7 User Parts (such as ISUP) over an IP network. M3UA is defined in RFC 4666.

M3UA uses SCTP as the transport layer. SCTP port 2905 is the expected port, although you can configure the signaling gateways to use a different port.

The MTP3 layer provides networking functions such as routing and node addressing, but uses point codes to identify nodes. The M3UA layer exchanges Originating Point Codes (OPC) and Destination Point Codes (DPC). This is similar to how IP uses IP addresses to identify nodes.

M3UA inspection provides limited protocol conformance. You can optionally apply access policy based on point codes or Service Indicators (SI). You can also apply rate limiting based on message class and type.

M3UA Protocol Conformance

M3UA inspection provides the following limited protocol enforcement. Inspection drops and logs packets that do not meet requirements.

- Common message header. Inspection validates all fields in the common header.
  - Version 1 only.
  - Message length must be correct.
  - Message type class with a reserved value is not allowed.
  - Invalid message ID within the message class is not allowed.
- Payload data message.
  - Only one parameter of a given type is allowed.
  - Data messages on SCTP stream 0 are not allowed.

M3UA Inspection Limitations

M3UA inspection has the following limitations.

- NAT is not supported for IP addresses embedded in M3UA data.
- Segmented M3UA messages will not be inspected and are likely to be dropped.
- SCTP does not support multi-homing or multi-streaming. If you need to support multi-homed flows you need to create access lists to allow them.
- Stateful failover is not supported for call flows and messages. Any failure occurring during a call flow might cause packets to be dropped and calls to be disconnected.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Policy Maps > Inspect > M3UA** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Configuring Class Maps for Inspection Policies, page 17-28

Field Reference

Table 17-60 Add and Edit M3UA Map Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Parameters tab	
SS7 Variant	Select the SS7 variant that will be used in your network for M3UA inspection.This option determines the valid format for point codes. After you configure the option and deploy an M3UA policy, you cannot change it unless you first remove the policy. The default SS7 variant is ITU.
Enable M3UA Application Server Process (ASP) State Validation	Select to perform application server process (ASP) state validation. The system maintains the ASP states of M3UA sessions and allows or drops ASP messages based on the validation result. If you do not enable strict ASP state validation, all ASP messages are forwarded uninspected.
Enforce Timeout	
Endpoint	Enter the idle timeout to remove statistics for an M3UA endpoint, in the hh:mm:ss format. To have no timeout, specify 0. The default is 30 minutes (00:30:00).
Session	Enter the idle timeout to remove an M3UA session if you enable strict ASP state validation, in hh:mm:ss format. To have no timeout, specify 0. The default value is 30 minutes (00:30:00). When this timeout is disabled, the system cannot remove stale sessions.

Table 17-60 Add and Edit M3UA Map Dialog Box (continued)

Element	Description
M3UA Message Tag Validation	
Specify, whether to check and validate the content of certain fields for the specified message type. Messages that fail validation are dropped. Validation differs by message type. Select the messages you want to validate.	
Destination User Part Unavailable (DUPU)	The User/Cause field must be present, and it must contain only valid cause and user codes.
Error	All mandatory fields must be present and must contain only allowed values. Each error message must contain the required fields for that error code.
Notify	The status type and status information fields must contain allowed values only.
Match Condition and Action Tab	
The Match All table lists the criteria included in the policy map. Each row indicates whether the inspection is looking for traffic that matches or does not match each criterion, the criterion and value that is inspected, and the action to be taken for traffic that satisfies the conditions. • To add a criterion, click the Add button and fill in the Match Condition and Action dialog box (see M3UA Policy Maps Add or Edit Match Condition and Action Dialog Boxes, page 17-105). • To edit a criterion, select it and click the Edit button. • To delete a criterion, select it and click the Delete button.	
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

M3UA Policy Maps Add or Edit Match Condition and Action Dialog Boxes

Use the Match Condition and Action dialog boxes to define the match criterion, value, and action directly in a M3UA policy map.

The fields on this dialog box change based on the criterion you select while creating a policy map.

Navigation Path

When creating a M3UA policy map, in the Policy Object Manager, from the Match Condition and Action tab on the Add and Edit M3UA Map dialog boxes, right-click inside the table, then select **Add Row** or right-click a row, then select **Edit Row**. See Configuring M3UA Maps, page 17-103.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22

Field Reference

Table 17-61 M3UA Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Criterion	Specifies which criterion of SCTP traffic to match - Message, DPC, OPC, or Service Indicator.
Message criterion	Matches the M3UA message class and type. The possible values for message class ID and its corresponding message ID are detailed here. Refer to the M3UA RFCs and documentation for detailed information about these messages. • class ID 0 (Management Messages)- message ID 0-1 • class ID 1(Transfer Messages)- message ID 1 • class ID 2(SS7 Signaling Network Management Messages)- message ID 1-6 • class ID 3(ASP State Maintenance Messages)-message ID 1-6 • class ID 4(ASP Traffic Maintenance Messages)- message ID 1-4 • class ID 9(Routing Key Management Messages)- message ID 1-4
DPC criterion	Matches the destination point code in the data message. Point code is in the zone-region-sp format, where the possible values for each element depend on the SS7 variant.
OPC criterion	Matches the originating point code in the data message, that is, the traffic source. Point code is in zone-region-sp format, where the possible values for each element depend on the SS7 variant: • ITU—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7]. • ANSI—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255]. • Japan—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127]. • China—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

Table 17-61 M3UA Policy Maps Add and Edit Match Condition and Action Dialog Boxes

Element	Description
Service Indicator criterion	Matches the service indicator number, 0-15. The available service indicators are listed in the variables section. Consult M3UA RFCs and documentation for detailed information about these service indicators • 0—Signaling Network Management Messages • 1—Signaling Network Testing and Maintenance Messages • 2—Signaling Network Testing and Maintenance Special Messages • 3—SCCP • 4—Telephone User Part • 5—ISDN User Part • 6—Data User Part (call and circuit-related messages) • 7—Data User Part (facility registration and cancellation messages) • 8—Reserved for MTP Testing User Part • 9—Broadband ISDN User Part • 10—Satellite ISDN User Part • 11—Reserved • 12—AAL type 2 Signaling • 13—Bearer Independent Call Control • 14—Gateway Control Protocol • 15—Reserved
Type	Specifies whether the map includes traffic that matches or does not match the criterion. For example, if Doesn't Match is selected on the string "example.com," then any traffic that contains "example.com" is excluded from the map. • Matches—Matches the criterion. • Doesn't Match—Does not match the criterion.
Action	The action you want the device to take for traffic that matches the defined criteria. • Drop Packet—By default, all invalid packets or packets that failed during parsing are dropped. • Drop Packet and Log— Same as drop packet and additionally send a system log message. • Rate Limit— Limit the rate of messages. This option is available when the message criterion is selected.

Configuring Regular Expression Groups

Use the Add and Edit Regular Expression Groups dialog boxes to define regular expression groups, which contain multiple regular expressions. Groups make it possible for you to create modular regular expressions and group them in multiple ways for various uses. The objects can be used in some inspection class maps and inspection policy maps.

Navigation Path

Select **Manage > Policy Objects**, then select **Maps > Regular Expressions Groups** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Creating Policy Objects, page 6-9

Field Reference

Table 17-62 Add and Edit Regular Expression Class Map Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Regular Expressions	The Regular Expression policy objects that include the expressions you want to include in the group. Enter the name of the objects or click **Select** to select them from a list or to create a new object.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add/Edit Regular Expressions

Use the Add and Edit Regular Expression dialog boxes to define regular expressions for use in class and policy inspection maps or in regular expression group policy objects. Regular expressions are also used in remote access SSL VPN client settings.

A regular expression matches text strings either literally as an exact string or by using metacharacters so you can match multiple variants of a text string. You can use regular expressions in various type of class and policy inspection maps to match various target items, for example, the content of certain application traffic such as the body text inside an HTTP packet.

Navigation Path

- Select **Manage > Policy Objects**, then select **Maps > Regular Expressions** from the Object Type selector. Right-click inside the work area, then select **New Object** or right-click a row and select **Edit Object**.
- From the Client Settings tab of the SSL VPN Other Settings policy for ASA devices, click the **Add Row** button for the AnyConnect Client Image table, or select an image and click the **Edit Row** button. For detailed information on opening the tab, see Configuring SSL VPN AnyConnect Client Settings (ASA), page 31-64. On the Add AnyConnect Client Image dialog box, click **Select** to open the Regular Expressions Selector dialog box. To add a new regular expression, click the **Add (+)** button on the Regular Expressions Selector dialog box.

Related Topics

- Understanding Map Objects, page 6-78
- Configuring Protocols and Maps for Inspection, page 17-22
- Creating Policy Objects, page 6-9

Field Reference

Table 17-63 Add and Edit Regular Expression Dialog Boxes

Element	Description
Name	The name of the policy object. A maximum of 40 characters is allowed.
Description	A description of the policy object. A maximum of 200 characters is allowed.
Value	The regular expression, up to 100 characters in length. For information on the metacharacters you can use to build regular expressions, see Metacharacters Used to Build Regular Expressions, page 17-109.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Metacharacters Used to Build Regular Expressions

The following table explains the metacharacters you can use to build regular expressions in the Add and Edit Regular Expression dialog boxes (see Add/Edit Regular Expressions, page 17-108).

Keep the following tips in mind when creating regular expressions:

- If you enter any metacharacters in your text string that you want to be used literally, add the backslash (\) escape character before them. For example, “example\.com”.
- If you want to match upper and lower case characters, enter text in both upper- and lowercase. For example, “cats” is entered as “[cC][aA][tT][sS]”.

Table 17-64 Metacharacters Used to Build Regular Expressions

Character	Description	Notes
.	Dot	Matches any single character. For example, d.g matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(exp)	Subexpression	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 abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, dog|cat matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, lo?se matches lse or lose.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, lo*se matches lse, lose, loose, etc.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, lo+se matches lose and loose, but not lse.
{x}	Repeat Quantifier	Repeat exactly x times. For example, ab(xy){3}z matches abxyxyxyz.
	Minimum repeat quantifier	Repeat at least x times. For example, ab(xy){2,}z matches abxyxyz, abxyxyxyz, etc.
[abc]	Character class	Matches any character in the brackets. For example, [abc] matches a, b, or c.
[^abc]	Negated character class	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.
[a-c]	Character range class	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 [-abc].
“”	Quotation marks	Preserves trailing or leading spaces in the string. For example, “ test” preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, \[matches the left square bracket.

Table 17-64 Metacharacters Used to Build Regular Expressions (continued)

Character	Description	Notes
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\xNN	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
\NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Configuring Settings for Inspection Rules for IOS Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX, FWSM, and IPS features/functionality, it does not support any enhancements.

If you configure inspection rules, you can also configure inspection settings to change the default settings for some global inspection parameters for IOS devices. Most of the inspection settings relate to preventing or mitigating Denial of Service (DoS) attacks. The default settings for most of these options are appropriate for most networks, so configure this policy only if you need to adjust one or more settings. If you do not change a setting, it is not configured on the device (the default remains configured).

To open the Inspection settings page, do one of the following:

- (Device view) Select a device, then select **Firewall > Settings > Inspection** from the Policy selector.
- (Policy view) Select **Firewall > Settings > Inspection** from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Settings > Inspection**.

The following table explains the available inspection settings.

Table 17-65 Inspection Page

Element	Description
Global Timeout Values	
TCP Establish Timeout (seconds)	How long to wait for a TCP session to reach the established state before dropping the session, in seconds, from 1-2147483. The default is 30.
FIN Wait Time (seconds)	How long to maintain TCP session state information after the firewall detects a FIN-exchange, in seconds, from 1-2147483. The FIN-exchange occurs when the TCP session is ready to close. The default is 5.

Table 17-65 Inspection Page (continued)

Element	Description
TCP Idle Time (seconds)	How long to maintain a TCP session while there is no activity in the session, in seconds, from 1-2147483. The default is 3600 (one hour).
UDP Idle Time (seconds)	How long to maintain a UDP session while there is no activity in the session, in seconds, from 1-2147483. The default is 30. When the software detects a valid UDP packet, the software establishes state information for a new UDP session. Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet. If the software detects no UDP packets for the UDP session for the period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.
DNS Timeout (seconds)	The length of time for which a DNS lookup session is managed while there is no activity, in seconds, from 1-2147483. The default is 5.
SYN Flooding DoS Attack Thresholds	
Maximum 1 Minute Connection Rate - low Maximum 1 Minute Connection Rate - high	The number of new unestablished sessions that causes the system to start and stop deleting half-open sessions. Ensure that you enter a lower number in the Low field than you enter in the High field. Possible values are from 1-2147483647 per minute. The default is 400 for low and 500 for high.
Maximum Incomplete Sessions Stop Threshold Maximum Incomplete Sessions Start Threshold	The number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions. Ensure that you enter a lower number in the stop field than you enter in the start field. Possible values are from 1-2147483647. The default is 400 for low and 500 for high.
Thresholds per Host	
Max Sessions Per Host	The number of half-open TCP sessions with the same host destination address that can exist at a time before the software starts deleting half-open sessions to the host. Possible values are 1-4294967295. The default is 50. A large number of half-open sessions can indicate there is a Denial of Service attack against the host.

Table 17-65 Inspection Page (continued)

Element	Description
Max Sessions Blocking Interval (min)	If the maximum sessions per host threshold is reached, the blocking time to apply to help mitigate the potential TCP host-specific denial-of-service (DoS) attack. Possible values are 0-35791 minutes. The default is 0. • If the blocking time value is 0, the software deletes the oldest existing half-open session for the host for every new connection request to the host above the maximum session limit. This ensures that the number of half-open sessions to a given host will never exceed the threshold. • If the blocking time value is greater than 0, the software deletes all existing half-open sessions for the host, then blocks all new connection requests to the host. The software will continue to block all new connection requests until the block-time expires.
Other	
Session Hash Table Size (buckets)	The size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192. The default is 1024. You should increase the hash table size when the total number of sessions running through the device is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.
Enable Alert Messages	Whether to generate stateful packet inspection alert messages on the console.
Enable Audit Trail Messages	Whether audit trail messages are logged to the syslog server or router.
Permit DHCP Passthrough (Transparent Firewall)	Whether to permit a transparent firewall to forward DHCP packets across the bridge without inspection. Permitting DHCP passthrough overrides an ACL for DHCP packets, so DHCP packets are forwarded even if the ACL is configured to deny all IP packets. Thus, clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.
Block Non-SYN Packets	Whether to drop TCP packets that do not belong to an established session. These are TCP packets that do not initiate sessions, that is, the SYN bit is not set in them.
Log Dropped Packets	Whether to create log messages for dropped packets to specify the reason for dropping them.

Related Topics

- Understanding Inspection Rules, page 17-2
- Configuring Inspection Rules, page 17-5
- Using Inspection To Prevent Denial of Service (DoS) Attacks on IOS Devices, page 17-5