CHAPTER 23

Managing Transparent Firewall Rules

Transparent firewall rules are access control rules for non-IP layer 2 traffic. You can use these rules to permit or drop traffic based on the Ethertype value in the layer-2 packet.

This chapter contains the following topics:

Configuring Transparent Firewall Rules

Transparent firewall rules are access control rules for non-IP layer 2 traffic. You can use these rules to permit or drop traffic based on the Ethertype value in the layer-2 packet. These rules create Ethertype access control lists on the device. With transparent rules, you can control the flow of non-IP traffic across the device. (To control IP traffic, use access rules; see Understanding Access Rules, page 16-1.)

Transparent firewalls are devices that you place within a single subnet to control traffic flow across a bridge. They allow you to insert a firewall on a subnet without renumbering your networks.

You can configure transparent rules only on the following types of interfaces:

- **IOS 12.3(7)T or later devices**—On layer-3 interfaces that are part of a bridge group:
  - Configure the interfaces you want to bridge as layer 3 in the **Interfaces > Interfaces** policy.
  - Configure a bridge group with two or more layer 3 interfaces in the **Platform > Device Admin > Bridging** policy (see Bridging on Cisco IOS Routers, page 63-18 and Defining Bridge Groups, page 63-20).
  - Create a bridge group virtual interface (BVI) using the same number as the bridge group (see Bridge-Group Virtual Interfaces, page 63-19). For example, if you create bridge group 12, create BVI12.
- **ASA, PIX 7.0+, FWSM devices**—On any interface when the device is running in transparent mode. If you are using multiple contexts, configure the rules on the individual security contexts.

  There are several other bridging policies that you can configure in the **Platform > Bridging** policy group including: ARP table and ARP inspection, MAC table and the ability to disable MAC learning, and the ability to configure a management IP address so that you can remotely manage the device. For more detail about transparent firewalls, see Chapter 47, "Configuring Bridging Policies on Firewall Devices" and Interfaces in Routed and Transparent Modes, page 46-5.

Tip On ASA, PIX, and FWSM in transparent mode, you must configure access rules to allow any IP traffic to pass through the device. Transparent rules control layer 2 non-IP traffic only.

Also, see NAT in Transparent Mode, page 24-16 for information about using network address translation on security devices.

You can also configure other types of firewall rules on these interfaces. The other types of rules apply to layer-3 and higher traffic.

Tip If you configure any transparent rule, an implicit **deny all** rule is added at the end of the rule list for each interface. You must ensure that you permit all desired traffic. You might want to include a **permit any** (for ASA/PIX/FWSM devices) or **permit 0x0000 0xFFFF** (for IOS devices) rule as the final rule in the table if your desire is simply to deny specific types of traffic, rather than permitting only specific types of traffic.

Related Topics

- Adding and Removing Rules, page 12-9
- Editing Rules, page 12-10
- Enabling and Disabling Rules, page 12-20

Step 1 Do one of the following to open the Transparent Rules Page, page 23-3:

- (Device view) Select **Firewall > Transparent Rules** from the Policy selector for a supported device type.
- (Policy view) Select **Firewall > Transparent 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 and Edit Transparent Firewall Rule Dialog Boxes, page 23-5.

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 Configure the rule. Following are the highlights of what you typically need to decide. For specific information on configuring the fields, see Add and Edit Transparent Firewall Rule Dialog Boxes, page 23-5.

- Permit or Deny—Whether you are allowing traffic that matches the rule or dropping it.
- Interfaces—The interface or interface role for which you are configuring the rule.
- The direction of traffic to which this rule should apply (in or out). The default is in.
- EtherType—The hexadecimal code or keyword (for ASA/PIX/FWSM only) that identifies the traffic. For a list of codes, see RFC 1700 at http://www.ietf.org/rfc/rfc1700.txt and search for "Ether Type." For ASA/PIX/FWSM, you can select a keyword to identify some EtherTypes. For ASA/PIX/FWSM, the code must be 0x0600 at minimum.
- Mask—For rules applied to IOS devices, you must also specify a mask to apply to the EtherType. Use 0xFFFF to have the EtherType interpreted literally.

If you want to create a single rule to apply to a group of EtherTypes, convert the EtherTypes to binary and calculate an appropriate mask where 1 means to interpret the EtherType literally, and 0 means that any value should be allowed in the position. You must then convert your mask into hexadecimal.

Click **OK** when you are finished defining your rule.

Step 4 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.

Step 5 (IOS devices only) If you are configuring transparent rules on an IOS device, you can forward DHCP traffic across the bridge without inspection. To configure this, select the **Firewall > Settings > Inspection** policy and select the **Permit DHCP Passthrough (Transparent Firewall)** option. This setting is not supported on all IOS versions, so carefully inspect validation results to see if it will be configured on your device.

Transparent Rules Page

Use the Transparent Rules page to control access for non-IP layer-2 traffic. (To control IP traffic access, use access rules; see Understanding Access Rules, page 16-1.)

Transparent rules are limited to transparent firewalls, which are ASA, PIX 7.0+, and FWSM devices running in transparent mode, or layer-3 interfaces that are part of a bridge group on IOS 12.3(7)T+ devices. When deployed, transparent rules become Ethertype access control lists.

Configure the same rules on all bridged interfaces to allow traffic to pass both ways through the device.

For more detailed information about configuring transparent firewalls and the device requirements for deploying these rules, see Configuring Transparent Firewall Rules, page 23-1.

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 Transparent Rules, do one of the following:

- (Device view) Select **Firewall > Transparent Rules** from the Policy selector for a supported device type.
- (Policy view) Select **Firewall > Transparent Rules** from the Policy Type selector. Select an existing policy or create a new one.
- (Map view) Right-click a device and select **Edit Firewall Policies > Transparent Rules**.

Related Topics

- Interfaces in Routed and Transparent Modes, page 46-5.
- Chapter 47, “Configuring Bridging Policies on Firewall Devices”
- Bridging on Cisco IOS Routers, page 63-18
- Defining Bridge Groups, page 63-20
- Bridge-Group Virtual Interfaces, page 63-19

- Filtering Tables, page 1-48

Field Reference

Table 23-1 Transparent Rules Page

Element	Description
No.	The ordered rule number.
Permit	Whether a rule permits or denies traffic based on the conditions set: • Permit—Shown as a green check mark. • Deny—Shown as a red circle with slash.
EtherType	The Ethernet packet type, which is the EtherType value in the packet. This can be a hexadecimal code or a keyword.
Mask	The 16-bit hexadecimal mask for the EtherType (for IOS devices only). A mask of 0xFFFF indicates the EtherType is literal. Any other mask indicates the corresponding bits in the EtherType to ignore. You must convert the hexadecimal number to binary to fully interpret the mask (binary 1 means interpret the corresponding EtherType value literally, 0 means allow any value at that position).
Interface	The interfaces or interface roles to which the rule is assigned. 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.
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.
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).
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 and Edit Transparent Firewall Rule Dialog Boxes, page 23-5. 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.

Table 23-1 Transparent Rules Page (continued)

Element	Description
Delete Row button	Click this button to delete the selected rule.

Add and Edit Transparent Firewall Rule Dialog Boxes

Use the Add and Edit Transparent Firewall Rule dialog boxes to add and edit transparent firewall rules, which are configured as EtherType access control lists on the device. Before you configure transparent rules, read Configuring Transparent Firewall Rules, page 23-1.

Navigation Path

From the Transparent Rules Page, page 23-3, click the **Add Row** button or select a row and click the **Edit Row** button.

Related Topics

- Interfaces in Routed and Transparent Modes, page 46-5.
- Chapter 47, "Configuring Bridging Policies on Firewall Devices"
- Bridging on Cisco IOS Routers, page 63-18
- Defining Bridge Groups, page 63-20
- Bridge-Group Virtual Interfaces, page 63-19
- Editing Rules, page 12-10
- Adding and Removing Rules, page 12-9

Field Reference

Table 23-2 Add and Edit Transparent Firewall Rule Dialog Boxes

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.
Action	Whether the rule permits or denies traffic based on the conditions you define.
Interfaces	The interfaces or interface roles to which the rule is assigned. You must select only bridged, transparent interfaces (for more specific information, see Configuring Transparent Firewall Rules, page 23-1). 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. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. See Understanding Interface Role Objects, page 6-73.

Table 23-2 Add and Edit Transparent Firewall Rule Dialog Boxes (continued)

Element	Description
Traffic Direction	The direction of the traffic to which this rule applies: • In—Packets entering an interface. • Out—Packets exiting an interface.
EtherType	The hexadecimal code or keyword (for ASA/PIX/FWSM only) that identifies the traffic based on the EtherType value in the packet. Enter or select the following: • The hexadecimal EtherType value. For a list of codes, see RFC 1700 at http://www.ietf.org/rfc/rfc1700.txt and search for "Ether Type." – IOS devices—You can enter any value from 0x0000 to 0xFFFF. – ASA/PIX/FWSM devices—The value must be 0x0600 or later. • For ASA/PIX/FWSM devices, you can also select these keywords: – bpdu—Spanning Tree Bridge Protocol Data Units – ipx—Internet Packet Exchange – mpls-unicast—Multi-Protocol Label Switching, unicast. – mpls-multicast—MPLS multicast. – isis—IS-IS pass-through – any—Any packet regardless of EtherType. – eii-ipx – raw-ipx **Tip** The keyword "isis" in the list above refers to IS-IS pass-through support, which is new in Security Manager 4.4. "IS-IS pass-through support" means that IS-IS traffic can flow through the ASA in transparent mode. **Note** Beginning from 4.16, the ethertype dsap CLI is used to interpret the installed ACEs—regardless of whether it was created with ether type bpdu, ipx, or isis— in ether type dsap format. This feature is supported for ASA 9.9(1) and later devices.
Wildcard Mask (IOS)	The mask is a 16-bit hexadecimal number that determines how the EtherType code is interpreted. A mask of 0xFFFF indicates the EtherType is literal. Any other mask indicates the corresponding bits in the EtherType to ignore. You must convert the hexadecimal number to binary to fully interpret the mask (binary 1 means interpret the corresponding EtherType value literally, 0 means allow any value at that position).
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).

Edit Transparent EtherType Dialog Box

Use the Edit Transparent EtherType dialog box to edit the EtherType in a transparent firewall rule. Enter the hexadecimal code that identifies the traffic. For ASA/PIX/FWSM devices, you can also select the keyword for some types of traffic. For a list of codes, see RFC 1700 at http://www.ietf.org/rfc/rfc1700.txt and search for "Ether Type." For a more detailed description of EtherType, see Add and Edit Transparent Firewall Rule Dialog Boxes, page 23-5.

For more information, see Configuring Transparent Firewall Rules, page 23-1.

Navigation Path

Right-click the EtherType cell in a transparent rule (on the Transparent Rules Page, page 23-3) and select **Edit EtherType**. You can edit the EtherType for one row at a time.

Edit Transparent Mask Dialog Box

Use the Edit Transparent Mask dialog box to edit the mask in a transparent firewall rule for an IOS device. The mask is a 16-bit hexadecimal number that determines how the EtherType code is interpreted.

A mask of 0xFFFF indicates the EtherType is literal. Any other mask indicates the corresponding bits in the EtherType to ignore. You must convert the hexadecimal number to binary to fully interpret the mask (binary 1 means interpret the corresponding EtherType value literally, 0 means allow any value at that position).

For more information, see Configuring Transparent Firewall Rules, page 23-1.

Navigation Path

Right-click the Mask cell in a transparent rule (on the Transparent Rules Page, page 23-3) and select **Edit Mask**. You can edit the mask for one row at a time.