Configuring Bridging Policies on Firewall Devices

This chapter contains the following topics:

About Bridging on Firewall Devices

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 device that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. The security appliance connects the same network on its inside and outside ports, acting as an access-control bridge; you assign different VLANs to each interface, and IP addressing is not used.

Thus, you can easily introduce a transparent firewall into an existing network—IP re-addressing is unnecessary—and maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

Although the transparent-mode device acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance unless you explicitly permit it with specific access rules. The only traffic allowed through a firewall without an access list is ARP traffic, which you can control using ARP inspection, and IPv6 neighbor discovery.

When the security appliance runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup. Route statements can still be configured, but they apply only to security appliance-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route so the security appliance can reach that subnet.

Starting from Cisco Security Manager 4.13, the Bridge-group Virtual Interface (BVI) feature is extended to the routed firewall mode. Routed firewalls are implemented by means of configuring bridge-groups. A user can configure up to eight bridge groups and on an ASA 9.7.1 (Cisco Security Manager 4.13) each group can contain upto 64 interfaces. On versions prior to Cisco Security Manager 4.13, a user can configure a maximum of two bridge groups; with each group containing a maximum limit of four interfaces. In addition to the BVI features supported in the transparent mode, the routed firewall mode includes support for the following additional communication modes:

- Inter BVI communication
- BVI to Data Port communication (Layer 2 to Layer 3) and vice versa

To configure a transparent firewall, use the following policies. When configuring an ASA/PIX/FWSM device in multiple-context mode, configure these policies on each transparent security context.

- **Firewall > Access Rules**—Access rules control layer 3 and higher traffic using extended access control lists. In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on access rules. Likewise, protocols like HSRP or VRRP can pass through the security appliance. However, the transparent-mode security appliance does not pass CDP packets.

  For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can provide those functions. For example, by using access rules, you can allow DHCP traffic to pass (instead of the unsupported DHCP relay feature), or multicast traffic such as that created by IP/TV.

  For more information, see Understanding Access Rules, page 16-1 and Configuring Access Rules, page 16-7.

- **Firewall > Transparent Rules**—Transparent rules control non-IP layer 2 traffic using Ethertype access control lists. For example, you can configure rules to allow AppleTalk, IPX, BPDUs, and MPLS to pass through the device. For more information, see Configuring Transparent Firewall Rules, page 23-1.

- **Platform > Bridging > ARP Table**, **ARP Inspection** and **IPv6 Neighbor Cache**—Use these policies to control the types of ARP and IPv6 traffic allowed through the bridge. If desired, you can configure static ARP and IPv6 neighbor cache entries and drop any traffic not defined by those static rules. Enable ARP inspection so that if a mismatch between the MAC address, the IP address, or the interface occurs, the security appliance drops the packet. This helps prevent ARP spoofing. For more information, see ARP Table Page, page 47-3 and ARP Inspection Page, page 47-5.

  Note The ARP Table and IPv6 Neighbor Cache are the only bridging policies available for non-transparent ASA/PIX/FWSM devices.

- **Platform > Bridging > MAC Address Table** and **MAC Learning**—Use these policies to configure static MAC-IP address mappings and to enable or disable MAC learning. MAC learning is enabled by default, which allows the appliance to add MAC-IP address mappings as traffic passes through the interface. If you want to prevent all traffic except from static entries, you can disable MAC learning. For more information, see MAC Address Table Page, page 47-7 and MAC Learning Page, page 47-8.

- **Platform > Bridging > Management IP** and **Platform > Bridging > Management IPv6**—Use these policies to configure a management IP address that Security Manager can use to communicate with the device.

Note The Management IP and Management IPv6 pages are not available on Catalyst 6500 service modules (the Firewall Services Module and the Adaptive Security Appliance Service Module).

If you change the management IP address, you also need to update the device properties for the device or security context. Follow these steps:

- Change the management IP address, save and submit your changes.
- Deploy your changes to the device.
- In Device view, select the device or security context, then select **Tools > Device Properties**. On the General page, enter the new management IP address in the IP Address field. On the Credentials tab, update the username and password fields with account credentials that can log into the management interface. Security Manager will now use this address and user account for subsequent deployments and device communication.

For more information, see Management IP Page, page 47-10.

Related Topics

- Bridging Support for FWSM 3.1, page 47-3
- Interfaces in Routed and Transparent Modes, page 46-5
- Transparent Rules Page, page 23-3

Bridging Support for FWSM 3.1

Although FWSM 3.1 can support multiple L2 interface pairs, Security Manager lets you specify no more than two L2 interfaces (a single interface pair), and one associated management IP address. That means only one bridge group with two named interfaces associated is provisioned with a management IP address. If the device configuration contains a maximum of one bridge group and two named interfaces, it is valid for discovery. All other scenarios result in an error message and the commands are ignored during discovery. Furthermore, discovery will not show any bridge-group information in Security Manager, although the bridge-group commands will be generated during deployment. Bridge group 1 will be deployed and used in transparent rule policies if no bridge group exists in the device configuration.

Related Topics

- About Bridging on Firewall Devices, page 47-1

ARP Table Page

Use the ARP Table page to add static ARP entries that map a MAC address to an IP address and identifies the interface through which the host is reached.

Navigation Path

- (Device view) Select **Platform > Bridging > ARP Table** from the Device Policy selector.

- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > ARP Table** from the Policy Type selector. Right-click **ARP Table** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Add/Edit ARP Configuration Dialog Box, page 47-4
- About Bridging on Firewall Devices, page 47-1
- ARP Inspection Page, page 47-5
- MAC Address Table Page, page 47-7
- MAC Learning Page, page 47-8
- Management IP Page, page 47-10

Field Reference

Table 47-1 ARP Table Page

Element	Description
Timeout (seconds)	The amount of time, between 60 and 4294967 seconds, before the security appliance rebuilds the ARP table. The default is 14400 seconds. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently. **Note** The timeout applies to the *dynamic* ARP table, and not the static entries contained in the ARP table.
ARP Table	
Interface	The interface to which the host is attached.
IP Address	The IP address of the host.
MAC Address	The MAC address of the host.
Alias Enabled	Indicates whether the security appliance performs proxy ARP for this mapping. If this setting is enabled and the security appliance receives an ARP request for the specified IP address, it responds with the security appliance MAC address. When the security appliance receives traffic destined for the host belonging to the IP address, the security appliance forwards the traffic to the host MAC address that you specify in this command. This feature is useful if you have devices that do not perform ARP, for example. **Note** In transparent firewall mode, this setting is ignored and the security appliance does not perform proxy ARP.

Add/Edit ARP Configuration Dialog Box

Use the Add/Edit ARP Configuration dialog box to add a static ARP entry that maps a MAC address to an IP address and identifies the interface through which the host is reached.

Navigation Path

You can access the Add/Edit ARP Configuration dialog box from the ARP Table page. For more information about the ARP Table page, see ARP Table Page, page 47-3.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3

Field Reference

Table 47-2 Add/Edit ARP Configuration dialog box

Element	Description
Interface	The name of the interface to which the host network is attached.
IP Address	The IP address of the host.
MAC Address	The MAC address of the host; for example, 00e0.1e4e.3d8b.
Enable Alias	When selected, enables proxy ARP for this mapping. If the security appliance receives an ARP request for the specified IP address, it responds with the security appliance MAC address. When the security appliance receives traffic destined for the host belonging to the IP address, the security appliance forwards the traffic to the host MAC address that you specify in this command. This feature is useful if you have devices that do not perform ARP, for example. **Note** In transparent firewall mode, this setting is ignored and the security appliance does not perform proxy ARP.

ARP Inspection Page

Use the ARP Inspection page to configure ARP inspection for a transparent firewall. ARP inspection is used to prevent ARP spoofing.

Navigation Path

- (Device view) Select **Platform > Bridging > ARP Inspection** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > ARP Inspection** from the Policy Type selector. Right-click **ARP Inspection** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Add/Edit ARP Inspection Dialog Box, page 47-6
- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3
- MAC Address Table Page, page 47-7
- MAC Learning Page, page 47-8
- Management IP Page, page 47-10

Field Reference

Table 47-3 ARP Inspection Page

Element	Description
ARP Inspection Table	
Interface	The name of the interface to which the ARP inspection setting applies.
ARP Inspection Enabled	Indicates whether ARP inspection is enabled on the specified interface.
Flood Enabled	Indicates whether packets that do not match any element of a static ARP entry should be flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, the security appliance drops the packet. If you do not select this check box, all non-matching packets are dropped. **Note** The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

Add/Edit ARP Inspection Dialog Box

Use the Add/Edit ARP Inspection dialog box to enable or disable ARP inspection for a transparent firewall interface.

Navigation Path

You can access the Add/Edit ARP Inspection dialog box from the ARP Inspection page. For more information about the ARP Inspection page, see ARP Inspection Page, page 47-5.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- ARP Inspection Page, page 47-5

Field Reference

Table 47-4 Add/Edit ARP Inspection dialog box

Element	Description
Interface	The name of the interface for which you are enabling or disabling ARP inspection.
Enable ARP Inspection on this interface	When selected, enables ARP inspection on the specified interface.
Flood ARP packets	When selected, packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, the security appliance drops the packet. If you do not select this check box, all non-matching packets are dropped. **Note** The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

Managing the IPv6 Neighbor Cache

Use the IPv6 Neighbor Cache page to manage static IPv6 neighbor entries that map a MAC address to an IPv6 address, and identify the interface through which the neighbor host is reached, to provide address-resolution functions for IPv6. This is available on ASA 7.0+ devices only.

Note The IPv6 Neighbor Cache entries are the IPv6 equivalent of the static ARP entries, managed on the ARP Table Page, page 47-3.

If an entry for a specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

The IPv6 Neighbor Cache page is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons. (These are standard buttons, as described in Using Tables, page 1-48.) The Add Row button opens the Add IPv6 Neighbor Cache Configuration dialog box, and Edit Row opens the Edit IPv6 Neighbor Cache Configuration dialog box. Other than the titles, the two dialog boxes are identical.

Note Ensure that IPv6 is enabled on at least one interface before trying to add a neighbor.

Field Reference

Table 47-5 Add/Edit IPv6 Neighbor Cache Configuration dialog boxes

Element	Description
Interface	Enter or Select the name of the interface on which to add the neighbor.
IP Address	Enter the IPv6 address that corresponds to the local data-link address. (If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.)
MAC Address	Enter the local data-line (hardware) MAC address of the host; for example, 00e0.1e4e.3d8b.

MAC Address Table Page

Use the MAC Address Table page to add static MAC address entries to the MAC Address table. The table associates the MAC address with the source interface so that the security appliance knows to send any packets addressed to the device out the correct interface.

Navigation Path

- (Device view) Select **Platform > Bridging > MAC Address Table** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > MAC Address Table** from the Policy Type selector. Right-click **MAC Address Table** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Add/Edit MAC Table Entry Dialog Box, page 47-8

- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3
- ARP Inspection Page, page 47-5
- MAC Learning Page, page 47-8
- Management IP Page, page 47-10

Field Reference

Table 47-6 MAC Address Table Page

Element	Description
Aging Time (minutes)	Sets the number of minutes, between 5 and 720 (12 hours), that a MAC address entry stays in the MAC address table before timing out. 5 minutes is the default.
MAC Address Table	
Interface	The interface to which the MAC address is associated.
MAC Address	The MAC address; for example, 00e0.1e4e.3d8b.

Add/Edit MAC Table Entry Dialog Box

Use the Add/Edit MAC Table Entry dialog box to add static MAC address entries to the MAC Address table or to modify entries in the MAC Address table.

Navigation Path

You can access the Add/Edit MAC Table Entry dialog box from the MAC Address Table page. For more information about the MAC Address Table page, see MAC Address Table Page, page 47-7.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- MAC Address Table Page, page 47-7

Field Reference

Table 47-7 Add/Edit MAC Table Entry dialog box

Element	Description
Interface	The interface to which the MAC address is associated.
MAC Address	The MAC address; for example, 00e0.1e4e.3d8b.

MAC Learning Page

Use the MAC Learning page to enable or disable MAC address learning on an interface. By default, each interface learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired; however, unless you statically add MAC addresses to the table, no traffic can pass through the security appliance.

Navigation Path

- (Device view) Select **Platform > Bridging > MAC Learning** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > MAC Learning** from the Policy Type selector. Right-click **MAC Learning** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Add/Edit MAC Learning Dialog Box, page 47-9
- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3
- ARP Inspection Page, page 47-5
- MAC Address Table Page, page 47-7
- Management IP Page, page 47-10

Field Reference

Table 47-8 MAC Learning Page

Element	Description
MAC Learning Table	
Interface	The interface to which the MAC learning setting applies.
MAC Learning Enabled	Indicates whether the security appliance learns MAC addresses from traffic entering the interface.

Add/Edit MAC Learning Dialog Box

Use the Add/Edit MAC Learning dialog box to enable or disable MAC address learning on an interface.

Navigation Path

You can access the Add/Edit MAC Learning dialog box from the MAC Learning page. For more information about the MAC Learning page, see MAC Learning Page, page 47-8.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- MAC Learning Page, page 47-8

Field Reference

Table 47-9 Add/Edit MAC Learning dialog box

Element	Description
Interface	The interface to which the MAC learning setting applies.
MAC Learning Enabled	When selected, the security appliance learns MAC addresses from traffic entering the interface.

Management IP Page

A transparent firewall does not participate in IP routing. The only IP configuration required for the device is specification of a management IP address, which is used as the source address for traffic originating on the device, such as system messages or communications with AAA servers. You can also use this address for remote-management access.

For IPv4 traffic, the management IP address is required to pass any traffic.

Note In addition to the management IP address for the device, you can configure an IP address for the Management 0/0 or 0/1 management-only interface. This IP address can be on a separate subnet from the main management IP address.

Use the Management IP page to set the management IP address for a security device, or for a context in transparent firewall mode.

Navigation Path

- (Device view) Select **Platform > Bridging > Management IP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > Management IP** from the Policy Type selector. Right-click **Management IP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3
- ARP Inspection Page, page 47-5
- MAC Address Table Page, page 47-7
- MAC Learning Page, page 47-8

Field Reference

Table 47-10 Management IP Page

Element	Description
Management IP Address	The management IP address.
Subnet Mask	The subnet mask that corresponds to the management IP address.

Management IPv6 Page (ASA 5505)

A transparent firewall does not participate in IP routing. The only IP configuration required for the device is specification of a management IP address, which is used as the source address for traffic originating on the device, such as system messages or communications with AAA servers. You can also use this address for remote-management access.

For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations. If you configure the global address, a link-local address is automatically configured on each interface, so you do not also need to specifically configure a link-local address.

However, if you do not configure a global management address, you need to configure interface link-local addresses, as described in Configuring IPv6 Interfaces (ASA/FWSM), page 46-47. Note that you can configure both IPv6 and IPv4 management addresses on a device.

On an ASA 5505 in transparent mode, use the Management IPv6 page to enable IPv6, configure neighbor solicitation, and manage IPv6 interface addresses.

Note This page is available only on ASA 5505 version 8.2 and 8.3 devices in transparent mode.

Navigation Path

- (Device view) Select **Platform > Bridging > Management IPv6** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Bridging > Management IPv6** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- About Bridging on Firewall Devices, page 47-1
- ARP Table Page, page 47-3
- ARP Inspection Page, page 47-5
- MAC Address Table Page, page 47-7
- MAC Learning Page, page 47-8

Field Reference

Table 47-11 Management IPv6 Page

Element	Description
Enable IPv6	Check this box to enable IPv6 and configure IPv6 management-interface addresses. You can deselect this option to disable IPv6, but retain the configuration information.

Table 47-11 Management IPv6 Page (continued)

Element	Description
DAD Attempts	To specify the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection (DAD), enter a number from 0 to 600 in this field. Entering 0 disables duplicate address detection. Entering 1 configures a single transmission without follow-up transmissions; this is the default. Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued: `%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside` If the duplicate address is a global address of the interface, the address is not used and an error message is issued, similar to that shown previously for a duplicate link-local address. All configuration commands associated with the duplicate address remain as-configured while the state of the address is set to DUPLICATE. If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address, and all other IPv6 address associated with the interface are regenerated (that is, duplicate address detection is performed only on the new link-local address).
NS Interval	The interval between IPv6 neighbor solicitation retransmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds; the default value is 1000 milliseconds.
Reachable Time	The amount of time, in milliseconds, within which a remote IPv6 node is considered still reachable, after initial reachability was confirmed. Valid values range from 0 to 3600000 milliseconds, the default value is 0. When 0 is used for the value, the reachable time is set as undetermined—it is up to the receiving devices to set and track reachable time. A configured time enables detection of unavailable neighbors. A shorter time allows detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.
Interface IPv6 Addresses	The IPv6 address(es) assigned to the management interface are listed in this table. Use the Add Row, Edit Row, and Delete Row buttons below this table to manage these entries. (These are standard buttons, as described in Using Tables, page 1-48.) Add Row and Edit Row open the IPv6 Address for Interface Dialog Box, page 46-52.