



CHAPTER 18

Firewall Mode Overview

This chapter describes how to set the firewall mode, as well as how the firewall works in each firewall mode. You can set the firewall mode independently for each context in multiple context mode.

The FWSM (or each context in multiple mode) can run in one of two firewall modes:

- Routed mode
- Transparent mode

This chapter includes the following sections:

- [Routed Mode Overview, page 18-1](#)
- [Transparent Mode Overview, page 18-1](#)
- [Setting Transparent or Routed Firewall Mode at the CLI, page 18-6](#)

Routed Mode Overview

In routed mode, the FWSM is considered to be a router hop in the network. It can use OSPF or passive RIP (in single context mode). Routed mode supports many interfaces, and each interface is on a different subnet. You can share interfaces between contexts, with some limitations.

The FWSM acts as a router between connected networks, and each interface requires an IP address on a different subnet. In single context mode, the routed firewall supports OSPF and RIP (in passive mode). Multiple context mode supports static routes only. We recommend using the advanced routing capabilities of the upstream and downstream routers instead of relying on the FWSM for extensive routing needs.

Transparent Mode Overview

A transparent firewall is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

This section describes transparent firewall mode, and includes the following topics:

- [Transparent Firewall Network, page 18-2](#)
- [Bridge Groups, page 18-2](#)
- [Allowing Layer 3 Traffic, page 18-2](#)
- [Allowed MAC Addresses, page 18-2](#)

- [Passing Traffic Not Allowed in Routed Mode, page 18-3](#)
- [MAC Address vs. Route Lookups, page 18-3](#)
- [Using the Transparent Firewall in Your Network, page 18-4](#)
- [Transparent Firewall Guidelines, page 18-5](#)
- [Unsupported Features in Transparent Mode, page 18-6](#)

Transparent Firewall Network

The FWSM connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; IP readdressing is unnecessary.

You can optionally enable NAT for hosts connected to the transparent firewall.

Bridge Groups

If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can configure up to eight pairs of interfaces, called bridge groups. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a system log server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; IP readdressing is unnecessary. Maintenance is facilitated because there are no complicated routing patterns to troubleshoot.

**Note**

Each bridge group requires a management IP address. The FWSM uses this IP address as the source address for packets originating from the bridge group. The management IP address must be on the same subnet as the connected network.

Allowing Layer 3 Traffic

Even though transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the FWSM unless you explicitly permit it with an extended access list. The only traffic allowed through the transparent firewall without an access list is ARP traffic. ARP traffic can be controlled by ARP inspection.

Allowed MAC Addresses

The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF

- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD
- Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the FWSM even if you allow it in an access list. The transparent firewall, however, can pass most types of traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).



Note

The transparent mode FWSM does not pass CDP packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported.

For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an extended access list. Likewise, protocols like HSRP or VRRP can pass through the FWSM.

Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType access list.

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 support the functionality. For example, by using an extended access list, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV.

MAC Address vs. Route Lookups

When the FWSM runs in transparent mode without NAT, 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 only apply to FWSM-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route so the FWSM can reach that subnet.

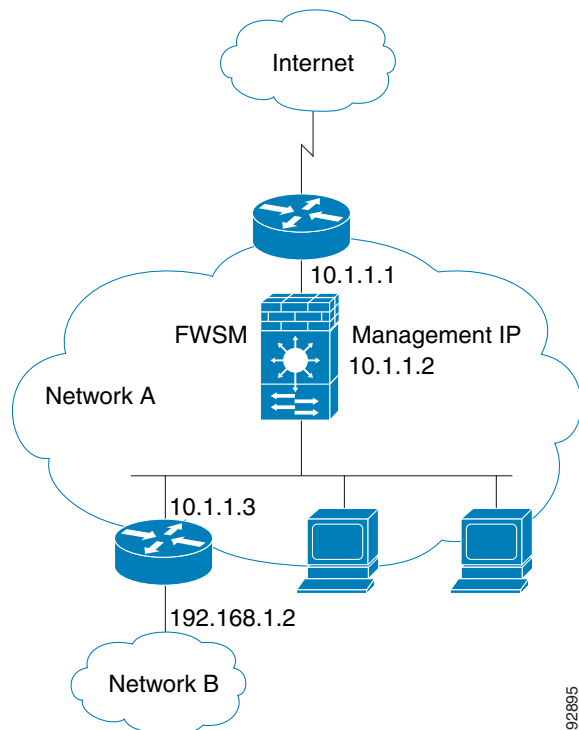
An exception to this rule is when you use voice inspections and the endpoint is at least one hop away from the FWSM. For example, if you use the transparent firewall between a CCM and an H.323 gateway, and there is a router between the transparent firewall and the H.323 gateway, then you need to add a static route on the FWSM for the H.323 gateway for successful call completion.

If you use NAT, then the FWSM uses a route lookup instead of a MAC address lookup. In some cases, you will need static routes. For example, if the real destination address is not directly-connected to the FWSM, then you need to add a static route on the FWSM for the real destination address that points to the downstream router.

Using the Transparent Firewall in Your Network

Figure 18-1 shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

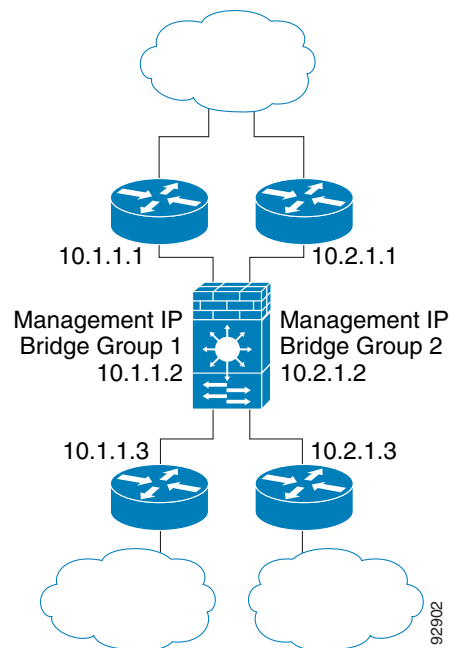
Figure 18-1 Transparent Firewall Network



92895

Figure 18-2 shows two networks connected to the FWSM, which has two bridge groups.

Figure 18-2 Transparent Firewall Network with Two Bridge Groups



Transparent Firewall Guidelines

Follow these guidelines when planning your transparent firewall network:

- A management IP address is required for each bridge group.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire bridge group. The FWSM uses this IP address as the source address for packets originating on the FWSM, such as system messages or AAA communications.

The management IP address must be on the same subnet as the connected network. See the [“Adding or Editing a Bridge Group”](#) section on page 8-3 for more information about management IP subnets.
- Each bridge group uses an inside interface and an outside interface only.
- Each directly-connected network must be on the same subnet.
- Do not specify the bridge group management IP address as the default gateway for connected devices; devices need to specify the router on the other side of the FWSM as the default gateway.
- The default route for the transparent firewall, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a static route that identifies the network from which you expect management traffic.
- For multiple context mode, each context must use different interfaces; you cannot share an interface across contexts.

- For multiple context mode, each context typically uses different subnets. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.
- You must use an extended access list to allow Layer 3 traffic, such as IP traffic, through the FWSM. You can also optionally use an EtherType access list to allow non-IP traffic through.

Unsupported Features in Transparent Mode

Table 18-1 lists features that are not supported in transparent mode.

Table 18-1 *Unsupported Features in Transparent Mode*

Unsupported Feature	Description
Dynamic routing protocols	You can, however, add static routes for traffic originating on the FWSM. You can also allow dynamic routing protocols through the FWSM using an extended access list.
IPv6 for the bridge group IP address	You can, however, pass the IPv6 EtherType using an EtherType access list.
DHCP relay	The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through using an extended access list.
LoopGuard on the switch	Do not enable LoopGuard globally on the switch if the FWSM is in transparent mode. LoopGuard is automatically applied to the internal EtherChannel between the switch and the FWSM, so after a failover and a failback, LoopGuard causes the secondary unit to be disconnected because the EtherChannel goes into the err-disable state.
Multicast	You can, however, allow multicast traffic through the FWSM by allowing it in an extended access list.
Remote access VPN for management	You can use site-to-site VPN for management.

Setting Transparent or Routed Firewall Mode at the CLI

You cannot change the mode in single mode in ASDM; in multiple mode, you cannot change the mode of the admin context in ASDM. You must change the mode at the CLI. You can set each context to run in routed firewall mode (the default) or transparent firewall mode.

When you change modes, the FWSM clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the FWSM that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the FWSM changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command is later in the configuration, the FWSM clears all the preceding lines in the configuration.

- To set the mode to transparent, enter the following command in each context:
hostname(config)# **firewall transparent**
- To set the mode to routed, enter the following command in each context:
hostname(config)# **no firewall transparent**

