



Configuring the Firewall Mode

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 5-1](#)
- [Transparent Mode Overview, page 5-8](#)
- [Setting Transparent or Routed Firewall Mode, page 5-16](#)

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.

- [IP Routing Support, page 5-1](#)
- [Network Address Translation, page 5-2](#)
- [How Data Moves Through the FWSM in Routed Firewall Mode, page 5-3](#)

IP Routing Support

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.

Network Address Translation

NAT substitutes the real address on a packet with a mapped address that is routable on the destination network. By default, NAT is not required. If you want to enforce a NAT policy that requires hosts on a higher security interface (inside) to use NAT when communicating with a lower security interface (outside), you can enable NAT control (see the **nat-control** command).



Note

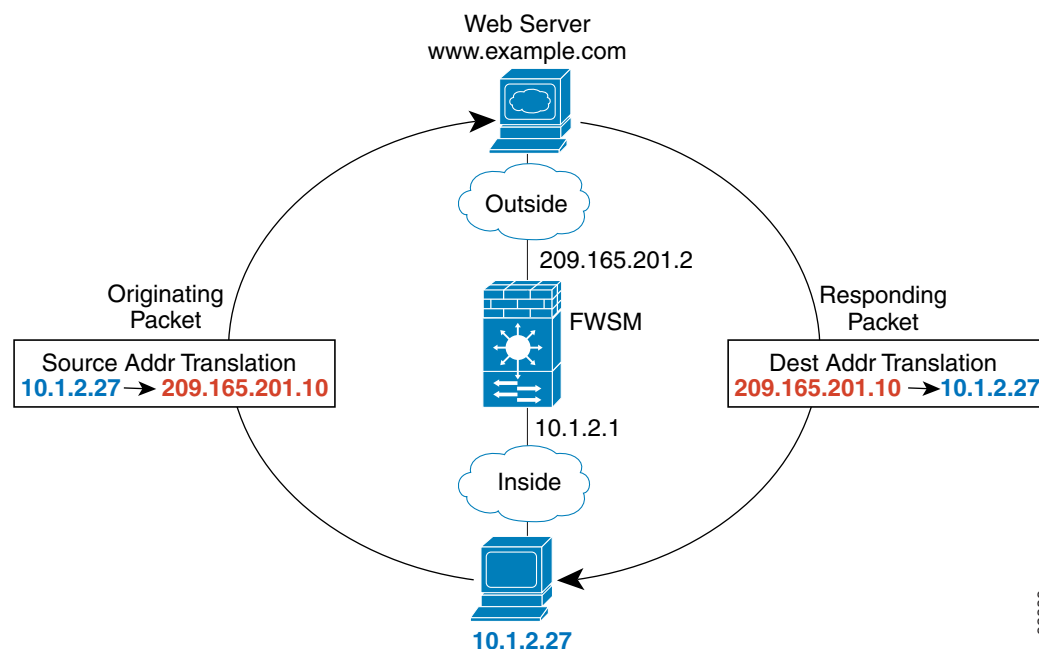
NAT control was the default behavior for software releases earlier than Version 3.1. If you upgrade an FWSM from an earlier version, then the **nat-control** command is automatically added to your configuration to maintain the expected behavior.

Some of the benefits of NAT include the following:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

Figure 5-1 shows a typical NAT scenario, with a private network on the inside. When the inside user sends a packet to a web server on the Internet, the local source address of the packet is changed to a routable global address. When the web server responds, it sends the response to the global address, and the FWSM receives the packet. The FWSM then translates the global address to the local address before sending it on to the user.

Figure 5-1 NAT Example



How Data Moves Through the FWSM in Routed Firewall Mode

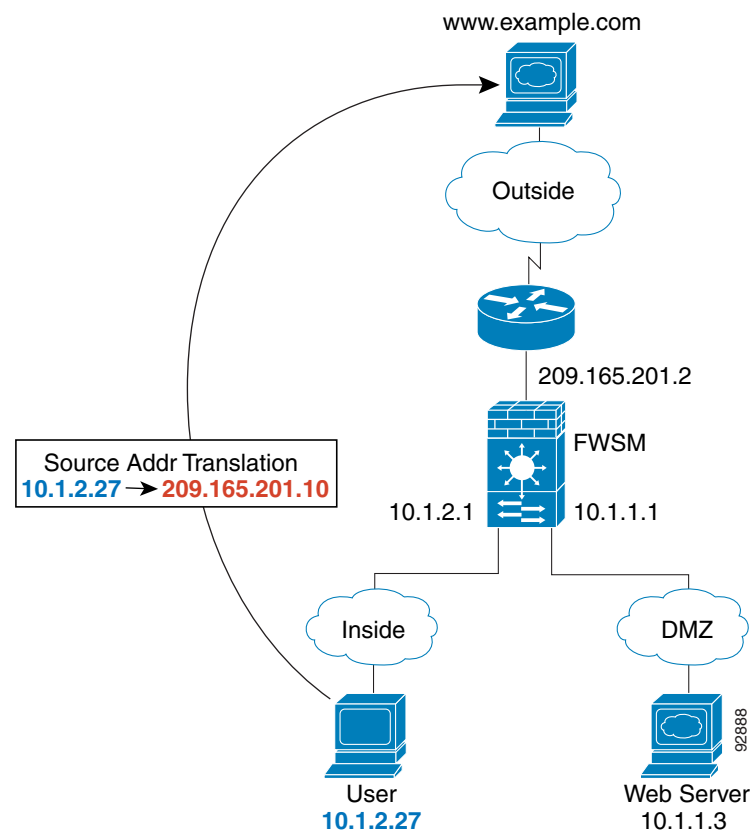
This section describes how data moves through the FWSM in routed firewall mode, and includes the following topics:

- [An Inside User Visits a Web Server, page 5-3](#)
- [An Outside User Visits a Web Server on the DMZ, page 5-4](#)
- [An Inside User Visits a Web Server on the DMZ, page 5-5](#)
- [An Outside User Attempts to Access an Inside Host, page 5-6](#)
- [A DMZ User Attempts to Access an Inside Host, page 5-7](#)

An Inside User Visits a Web Server

Figure 5-2 shows an inside user accessing an outside web server.

Figure 5-2 *Inside to Outside*



The following steps describe how data moves through the FWSM (see Figure 5-2):

1. The user on the inside network requests a web page from www.example.com.
2. The FWSM receives the packet and because it is a new session, the FWSM verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the FWSM first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface would be unique; the `www.example.com` IP address does not have a current address translation in a context.

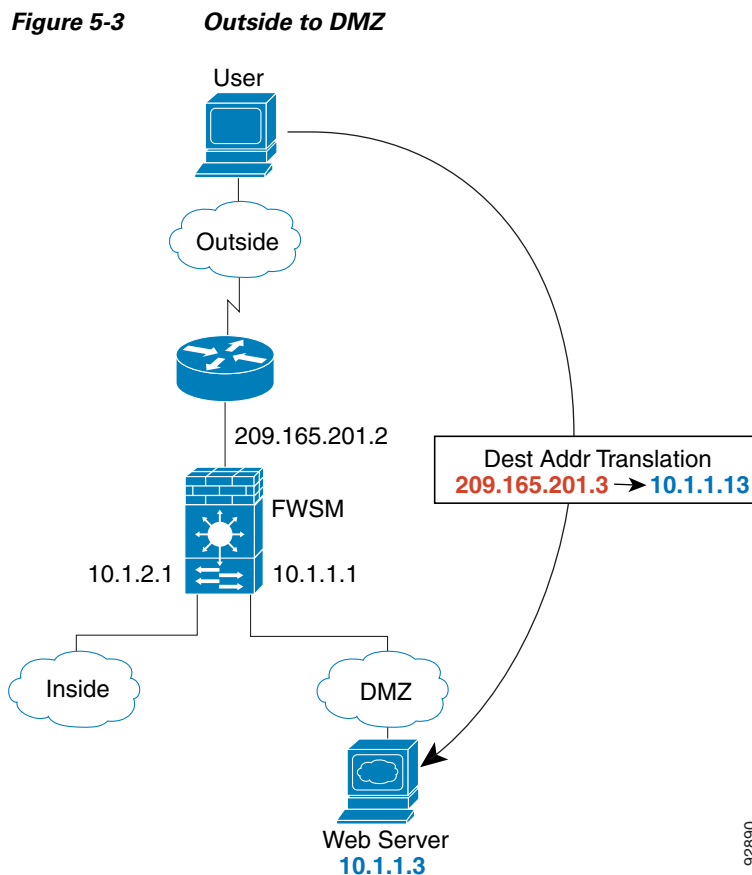
3. The FWSM translates the real address (10.1.2.27) to the mapped address 209.165.201.10, which is on the outside interface subnet.

The mapped address could be on any subnet, but routing is simplified when it is on the outside interface subnet.

4. The FWSM then records that a session is established and forwards the packet from the outside interface.
5. When `www.example.com` responds to the request, the packet goes through the FWSM, and because the session is already established, the packet bypasses the many lookups associated with a new connection. The FWSM performs NAT by translating the mapped address to the real address, 10.1.2.27.
6. The FWSM forwards the packet to the inside user.

An Outside User Visits a Web Server on the DMZ

Figure 5-3 shows an outside user accessing the DMZ web server.



The following steps describe how data moves through the FWSM (see [Figure 5-3](#)):

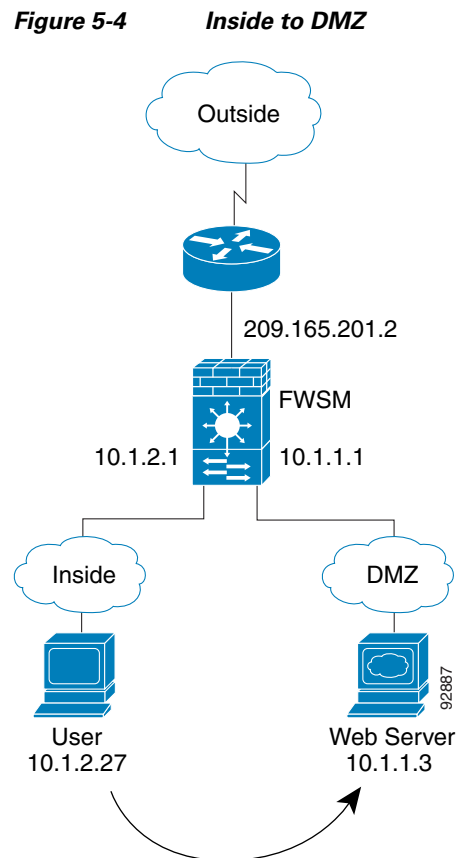
1. A user on the outside network requests a web page from the DMZ web server using the mapped address of 209.165.201.3, which is on the outside interface subnet.
2. The FWSM receives the packet and because it is a new session, the FWSM verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the FWSM first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the classifier “knows” that the DMZ web server address belongs to a certain context because of the server address translation.

3. The FWSM translates the destination address to the real address 10.1.1.3.
4. The FWSM then adds a session entry to the fast path and forwards the packet from the DMZ interface.
5. When the DMZ web server responds to the request, the packet goes through the FWSM and because the session is already established, the packet bypasses the many lookups associated with a new connection. The FWSM performs NAT by translating the real address to 209.165.201.3.
6. The FWSM forwards the packet to the outside user.

An Inside User Visits a Web Server on the DMZ

[Figure 5-4](#) shows an inside user accessing the DMZ web server.



The following steps describe how data moves through the FWSM (see [Figure 5-4](#)):

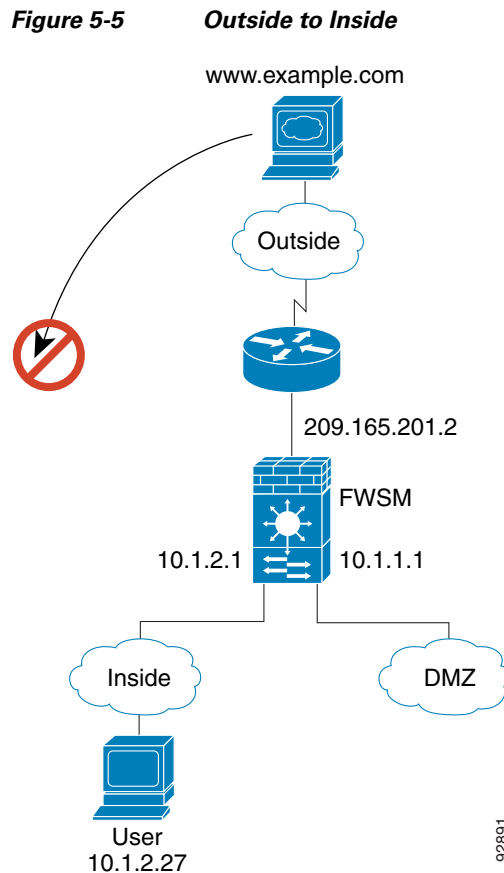
1. A user on the inside network requests a web page from the DMZ web server using the destination address of 10.1.1.3.
2. The FWSM receives the packet and because it is a new session, the FWSM verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the FWSM first classifies the packet according to either a unique interface or a unique destination address associated with a context; the destination address is associated by matching an address translation in a context. In this case, the interface is unique; the web server IP address does not have a current address translation.

3. The FWSM then records that a session is established and forwards the packet out of the DMZ interface.
4. When the DMZ web server responds to the request, the packet goes through the fast path, which lets the packet bypass the many lookups associated with a new connection.
5. The FWSM forwards the packet to the inside user.

An Outside User Attempts to Access an Inside Host

[Figure 5-5](#) shows an outside user attempting to access the inside network.

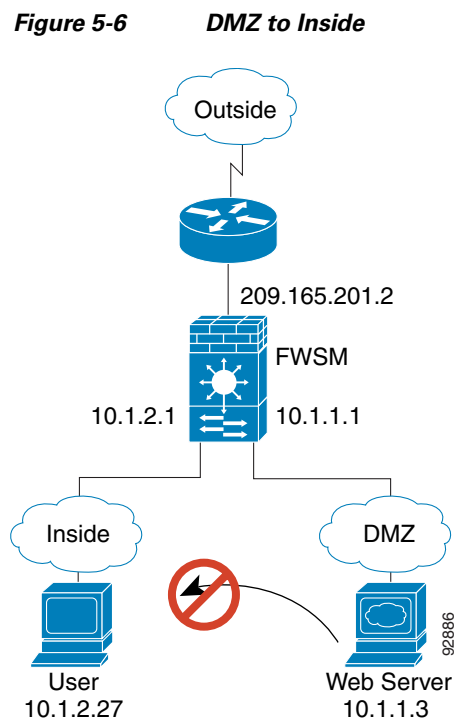


The following steps describe how data moves through the FWSM (see [Figure 5-5](#)):

1. A user on the outside network attempts to reach an inside host (assuming the host has a routable IP address).
If the inside network uses private addresses, no outside user can reach the inside network without NAT. The outside user might attempt to reach an inside user by using an existing NAT session.
2. The FWSM receives the packet and because it is a new session, the FWSM verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
3. The packet is denied, and the FWSM drops the packet and logs the connection attempt.
If the outside user is attempting to attack the inside network, the FWSM employs many technologies to determine if a packet is valid for an already established session.

A DMZ User Attempts to Access an Inside Host

[Figure 5-6](#) shows a user in the DMZ attempting to access the inside network.



The following steps describe how data moves through the FWSM (see [Figure 5-6](#)):

1. A user on the DMZ network attempts to reach an inside host. Because the DMZ does not have to route the traffic on the Internet, the private addressing scheme does not prevent routing.
2. The FWSM receives the packet and because it is a new session, the FWSM verifies if the packet is allowed according to the security policy (access lists, filters, AAA).
3. The packet is denied, and the FWSM drops the packet and logs the connection attempt.

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 5-8](#)
- [Bridge Groups, page 5-8](#)
- [Allowing Layer 3 Traffic, page 5-9](#)
- [Allowed MAC Addresses, page 5-9](#)
- [Passing Traffic Not Allowed in Routed Mode, page 5-9](#)
- [MAC Address vs. Route Lookups, page 5-9](#)
- [Using the Transparent Firewall in Your Network, page 5-10](#)
- [Transparent Firewall Guidelines, page 5-11](#)
- [Unsupported Features in Transparent Mode, page 5-12](#)
- [How Data Moves Through the Transparent Firewall, page 5-13](#)

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.

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 and no NAT configuration.

**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. See [Table 10-2 on page 10-6](#) for more information about allowing special traffic.

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

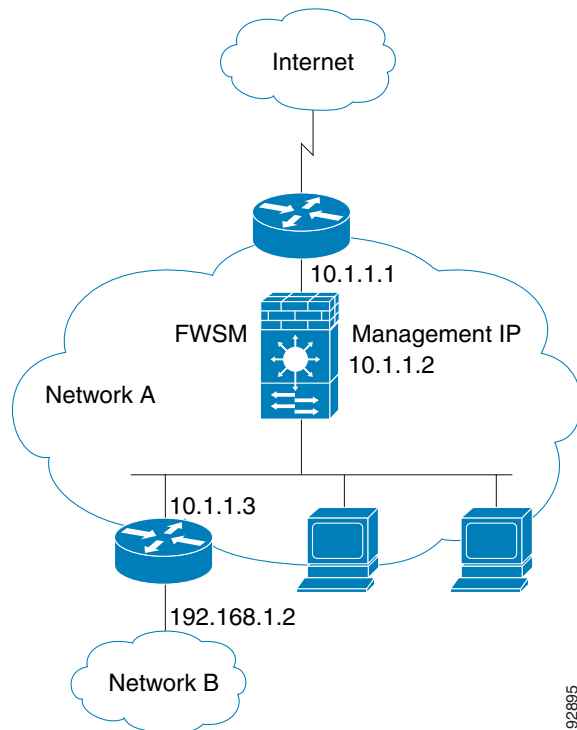
When the FWSM runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup. Route statements can still be configured, but they only apply to FWSM-originated traffic. For example, if your syslog server is located on a remote network,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

Using the Transparent Firewall in Your Network

Figure 5-7 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.

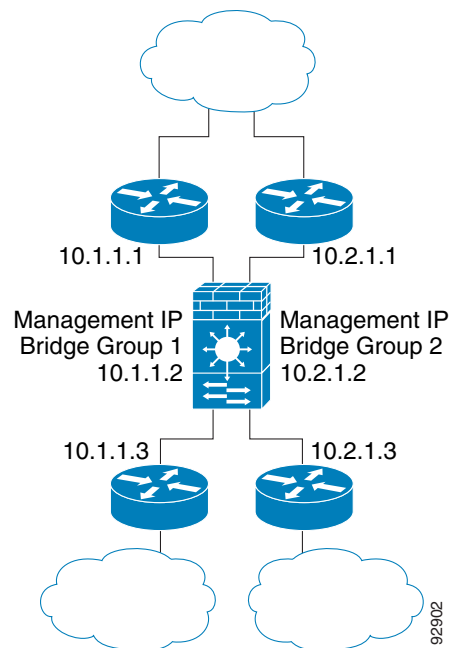
Figure 5-7 Transparent Firewall Network



92895

Figure 5-8 shows two networks connected to the FWSM, which has two bridge groups.

Figure 5-8 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. The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported. See the “[Assigning an IP Address to a Bridge Group](#)” section on page 6-5 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 5-1 lists features that are not supported in transparent mode.

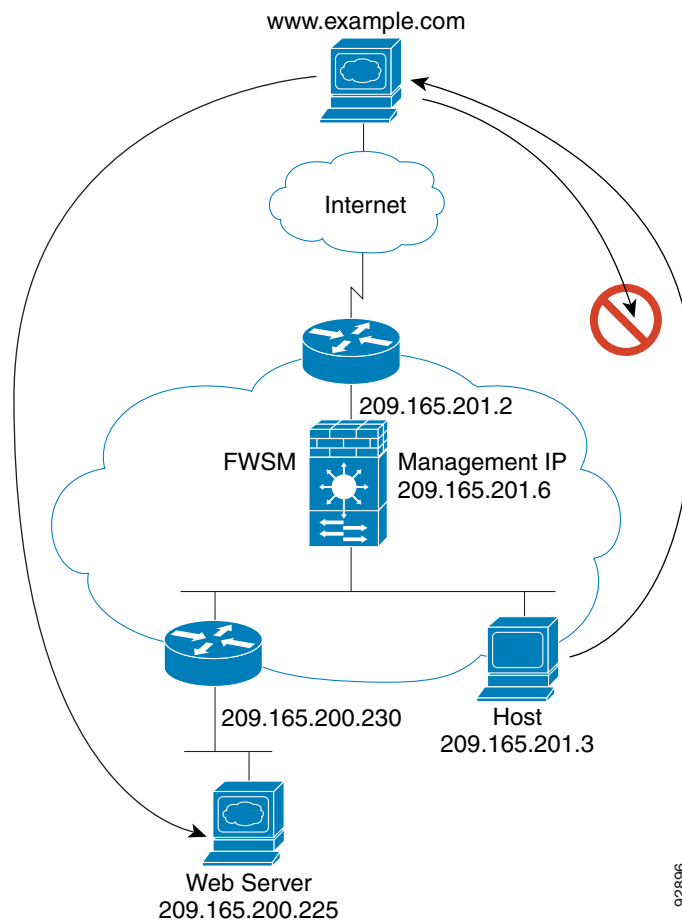
Table 5-1 *Unsupported Features in Transparent Mode*

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.
Multicast	You can, however, allow multicast traffic through the FWSM by allowing it in an extended access list.
NAT	NAT is performed on the upstream router.
Remote access VPN for management	You can use site-to-site VPN for management.
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.

How Data Moves Through the Transparent Firewall

Figure 5-9 shows a typical transparent firewall implementation with an inside network that contains a public web server. The FWSM has an access list so that the inside users can access Internet resources. Another access list lets the outside users access only the web server on the inside network.

Figure 5-9 Typical Transparent Firewall Data Path



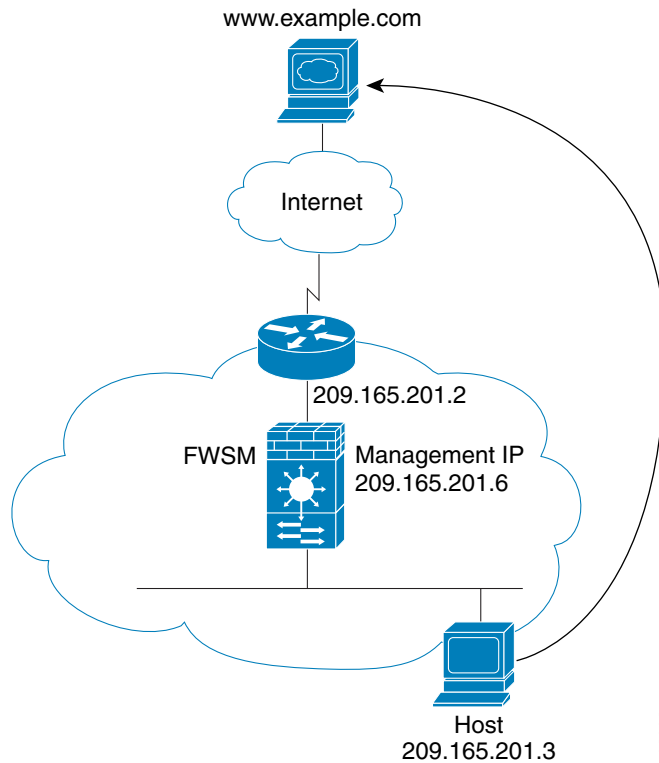
This section describes how data moves through the FWSM, and includes the following topics:

- [An Inside User Visits a Web Server, page 5-14](#)
- [An Outside User Visits a Web Server on the Inside Network, page 5-15](#)
- [An Outside User Attempts to Access an Inside Host, page 5-16](#)

An Inside User Visits a Web Server

Figure 5-10 shows an inside user accessing an outside web server.

Figure 5-10 *Inside to Outside*



The following steps describe how data moves through the FWSM (see Figure 5-10):

1. The user on the inside network requests a web page from www.example.com.
2. The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

For multiple context mode, the FWSM first classifies the packet according to a unique interface.

3. The FWSM records that a session is established.
4. If the destination MAC address is in its table, the FWSM forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 209.165.201.2.

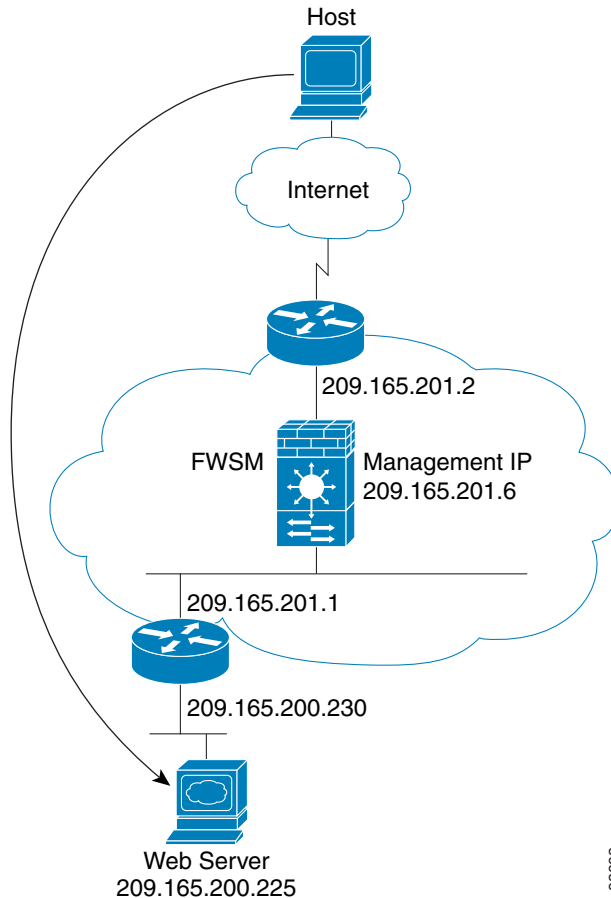
If the destination MAC address is not in the FWSM table, the FWSM attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.

5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The FWSM forwards the packet to the inside user.

An Outside User Visits a Web Server on the Inside Network

Figure 5-11 shows an outside user accessing the inside web server.

Figure 5-11 *Outside to Inside*



The following steps describe how data moves through the FWSM (see Figure 5-11):

1. A user on the outside network requests a web page from the inside web server.
2. The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (access lists, filters, AAA).

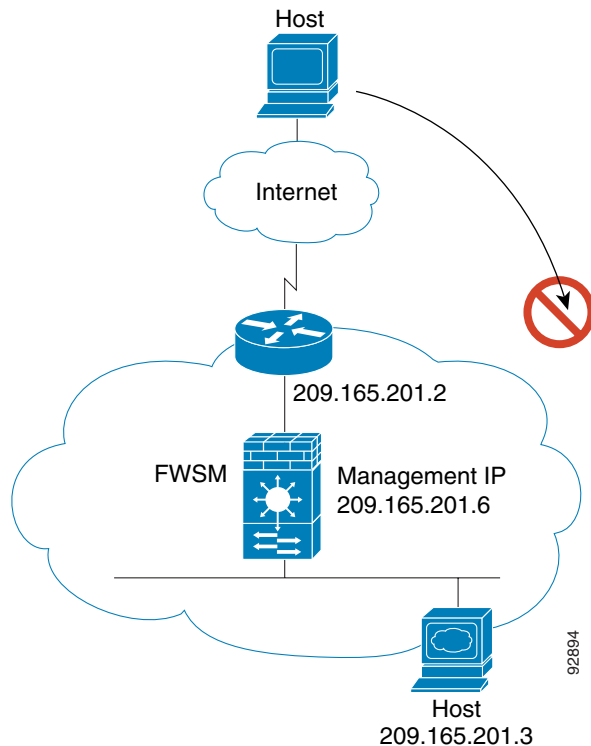
For multiple context mode, the FWSM first classifies the packet according to a unique interface.

3. The FWSM records that a session is established.
4. If the destination MAC address is in its table, the FWSM forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 209.186.201.1.
If the destination MAC address is not in the FWSM table, the FWSM attempts to discover the MAC address by sending an ARP request and a ping. The first packet is dropped.
5. The web server responds to the request; because the session is already established, the packet bypasses the many lookups associated with a new connection.
6. The FWSM forwards the packet to the outside user.

An Outside User Attempts to Access an Inside Host

Figure 5-12 shows an outside user attempting to access a host on the inside network.

Figure 5-12 *Outside to Inside*



The following steps describe how data moves through the FWSM (see Figure 5-12):

1. A user on the outside network attempts to reach an inside host.
2. The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies if the packet is allowed according to the terms of the security policy (access lists, filters, AAA).
For multiple context mode, the FWSM first classifies the packet according to a unique interface.
3. The packet is denied, and the FWSM drops the packet.
4. If the outside user is attempting to attack the inside network, the FWSM employs many technologies to determine if a packet is valid for an already established session.

Setting Transparent or Routed Firewall Mode

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
```

