Configuring the Firewall Mode

This chapter describes how to set the firewall mode to either routed mode or transparent mode, and includes the following sections:

Firewall Mode Overview

The FWSM can run in two firewall modes:

- Routed mode
- Transparent mode

In routed mode, the FWSM is considered to be a router hop in the network. It performs NAT between connected networks, and can use OSPF or passive RIP (in single context mode). Routed mode supports up to 256 interfaces per context or in single mode, with a maximum of 1000 interfaces divided between all contexts. Each interface is on a different subnet. You can share interfaces between contexts.

In transparent mode, the FWSM acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The FWSM connects the same network on its inside and outside interfaces, but each interface must be on a different VLAN. No dynamic routing protocols or NAT are required. However, like routed mode, transparent mode also requires ACLs to allow any traffic through aside from ARP packets. Transparent mode can allow certain types of traffic in an ACL that are blocked by routed mode, including unsupported routing protocols and multicast traffic. Transparent mode can also optionally use EtherType ACLs to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface.

This section includes the following topics:

Routed Mode Overview

This section includes the following topics:

- How Data Moves Through the FWSM in Routed Firewall Mode, page 4-3

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, such as the MSFC, instead of relying on the FWSM for extensive routing needs.

Network Address Translation

NAT substitutes the local address on a packet with a global address that is routable on the destination network. In routed mode, you typically configure NAT for inside hosts that access an outside network, but you can optionally bypass NAT if you are using routable addresses.

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. See the "Private Networks" section on page D-2 for more information.

- 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 4-1 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 firewall receives the packet. The firewall then translates the global address to the local address before sending it on to the user.

See Chapter 9, "Configuring Network Address Translation," for more information.

Figure 4-1   NAT Example
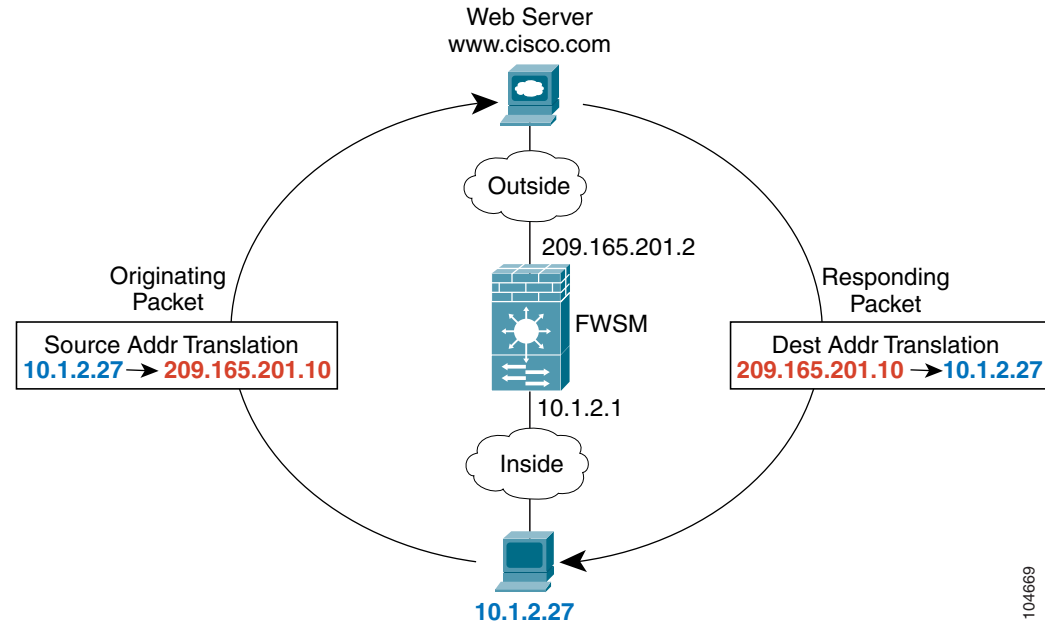
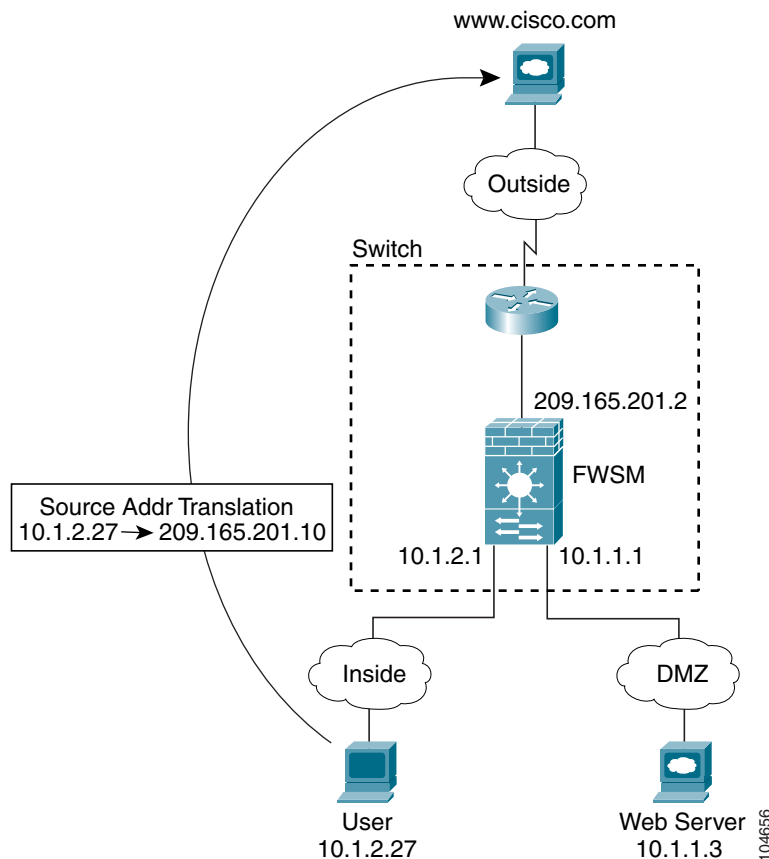## How Data Moves Through the FWSM in Routed Firewall Mode

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

- An Inside User Visits a Website, page 4-4
- An Outside User Visits a Website on the DMZ, page 4-5
- An Inside User Visits a Website on the DMZ, page 4-6
- An Outside User Attempts to Access an Inside Host, page 4-7
- An DMZ User Attempts to Access an Inside Host, page 4-8

An Inside User Visits a Website

Figure 4-2 shows an inside user accessing an outside website.

Figure 4-2   Inside to Outside

The steps below describe how data moves through the FWSM (see Figure 4-2):

1. The user on the inside network requests a web page from www.cisco.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 (ACLs, filters, AAA).

   For multiple context mode, the FWSM first classifies the packet according to either a unique VLAN or a unique destination address. In this case, the VLAN would be unique; the www.cisco.com IP address is not located uniquely within a context and is not a unique destination address.

3. The FWSM translates the local source address (10.1.2.27) to the global address 209.165.201.10, which is on the outside interface subnet.

   The global 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.cisco.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 fast path performs NAT by translating the global destination address to the local user address, 10.1.2.27.

6. The FWSM forwards the packet to the inside user.

An Outside User Visits a Website on the DMZ

Figure 4-3 shows an outside user accessing the DMZ website.
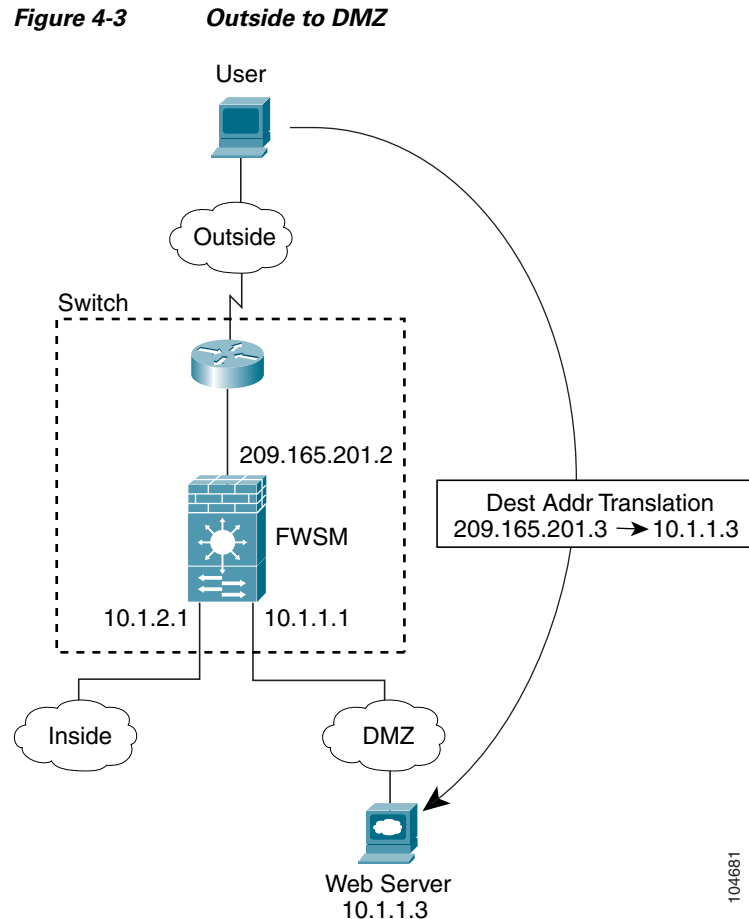
Figure 4-3   *Outside to DMZ*

The steps below describe how data moves through the FWSM (see Figure 4-3):

1. A user on the outside network requests a web page from the DMZ website using the global destination 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 (ACLs, filters, AAA).

   For multiple context mode, the FWSM first classifies the packet according to either a unique VLAN or a unique destination address. In this case, even if the VLAN is not unique, the classifier "knows" that the DMZ web server address belongs to a certain context because of the NAT configuration.
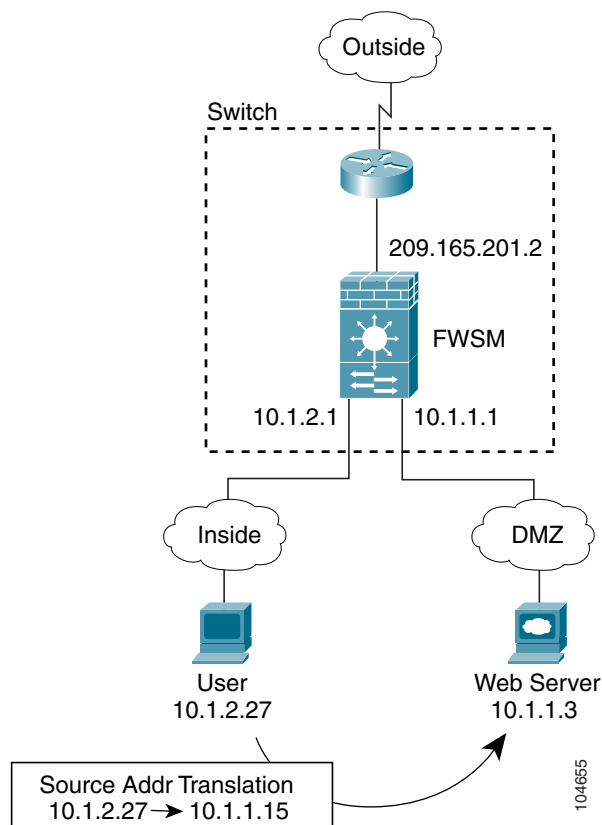
3. The FWSM translates the destination address to the local address 10.1.1.3.

4. The FWSM then adds a session entry to the fast path and forwards the packet from the DMZ interface.

5. When the DMZ website 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 fast path performs NAT by translating the local source address to 209.165.201.3.

6. The FWSM forwards the packet to the outside user.

An Inside User Visits a Website on the DMZ

Figure 4-4 shows an inside user accessing the DMZ website.

Figure 4-4   Inside to DMZ

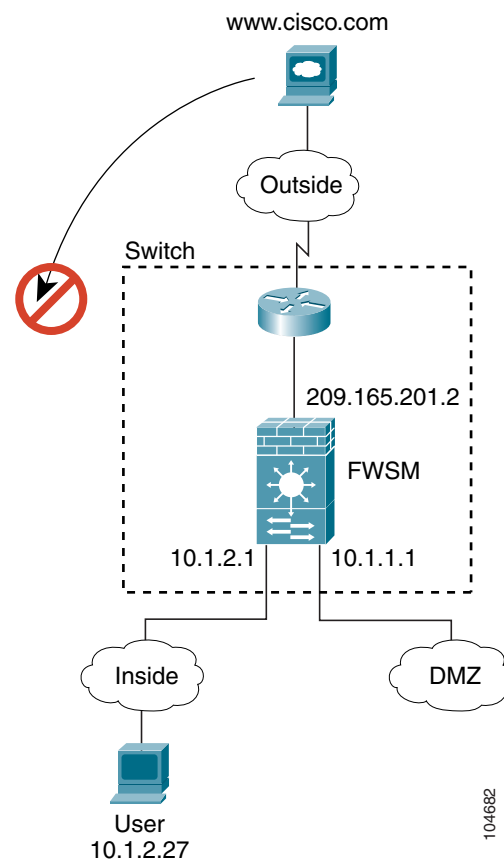The steps below describe how data moves through the FWSM (see Figure 4-4):

1. A user on the inside network requests a web page from the DMZ website using the destination address of 10.1.1.3.

   Because the DMZ is a lower security interface, the inside user can use the untranslated local address of the web server.

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 (ACLs, filters, AAA).

   For multiple context mode, the FWSM first classifies the packet according to either a unique VLAN or a unique destination address. In this case, the VLAN would be unique because the destination is on a different interface in the same context.

3. The FWSM translates the local source address to the global address 10.1.1.15, which is on the DMZ subnet.

4. The FWSM then records that a session is established and forwards the packet out of the DMZ interface.

5. When the DMZ web server responds to the request, the packet goes through the fast path, which allows the packet to bypass the many lookups associated with a new connection. The fast path performs NAT by translating the global destination address to the local address of the user, 10.1.2.27.

6. The FWSM forwards the packet to the inside user.

An Outside User Attempts to Access an Inside Host

Figure 4-5 shows an outside user attempting to access the inside network.

Figure 4-5   *Outside to Inside*

The steps below describe how data moves through the FWSM (see Figure 4-5):

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.
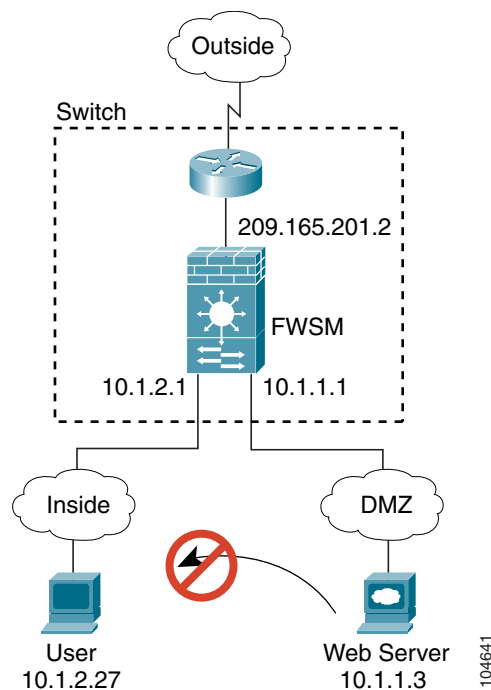
2. The FWSM receives the packet, and because it is a new session, the FWSM verifies if the packet is allowed according to the security policy (ACLs, filters, AAA).

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. See the "Other Protection Features" section on page 1-6 for more information.

An DMZ User Attempts to Access an Inside Host

Figure 4-6 shows a user in the DMZ attempting to access the inside network.

Figure 4-6   DMZ to Inside

The steps below describe how data moves through the FWSM (see Figure 4-6):

1. A user on the DMZ network attempts to reach an inside host. The DMZ host might know the real address of an inside host, and 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 (ACLs, filters, AAA).

3. The packet is denied, and the FWSM drops the packet and logs the connection attempt.

Transparent Mode Overview

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

- Transparent Firewall Features, page 4-9
- Using the Transparent Firewall in Your Network, page 4-10

Transparent Firewall Features

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 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. The Firewall Services Module (FWSM) connects the same network on its inside and outside ports but uses different VLANs on the inside and outside.

Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network. You assign different VLANs to each interface, and IP readdressing is unnecessary.

Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

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 control list (ACL). (See the "Adding an Extended Access Control List" section on page 10-13.) The only traffic allowed through the transparent firewall without an ACL is ARP traffic. ARP traffic can be controlled by ARP inspection (see the "Configuring ARP Inspection" section on page 7-3 for more information).

In routed mode, some types of traffic cannot pass through the FWSM even if you allow it in an ACL. The transparent firewall, however, can allow any traffic through using either an extended ACL (for IP traffic) or an EtherType ACL (for non-IP traffic). See the "Adding an EtherType Access Control List" section on page 10-16 for more information.

Note The transparent mode FWSM does not pass Cisco Discovery Protocol (CDP) packets.

For example, you can allow multicast traffic such as that created by IPTV using an extended ACL. You can also establish routing protocol adjacencies through a transparent firewall; for example, you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an extended ACL. Likewise, protocols like HSRP or VRRP can pass through the FWSM.

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

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. See the "Configuring Static Routes" section on page 8-3 for more information.

Using the Transparent Firewall in Your Network

Figure 4-7 shows a typical transparent firewall network. While the outside devices are on the same subnet as the inside devices, the VLANs are different. The inside router and hosts appear to be directly connected to the outside router. However, no traffic can bypass the FWSM because it must route between the two VLANs.

Figure 4-7   Transparent Firewall Network
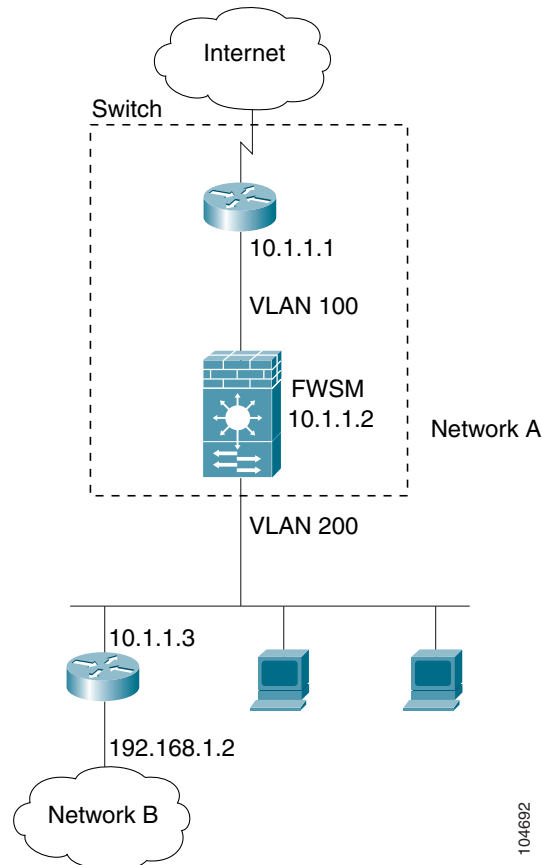
Transparent Firewall Guidelines

Follow these guidelines when planning your transparent firewall network:

- The transparent FWSM uses an inside interface and an outside interface only.

- Each directly connected network must be on the same subnet.

- A management IP address is required for each context, even if you do not intend to use Telnet to the context.

  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.

- Do not specify the FWSM 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.

- Each interface must be a different VLAN interface.

- For multiple context mode, each context must use different VLANs; you cannot share a VLAN across contexts.

- For multiple context mode, each context can use the same (overlapping) subnet or different subnets. Make sure that the upstream router performs NAT if you use overlapping subnets.

- Dynamic routing protocols are neither required nor supported.

  You can, however, add static routes.

- NAT is not supported.

  NAT is performed on the upstream router. However, you can configure some parameters available only in the **static** command. See the "Configuring Connection Limits for Non-NAT Configurations" section on page 6-9 for more information.

- You must use an extended ACL to allow Layer 3 traffic, such as IP traffic, through the FWSM.

  You can also optionally use an EtherType ACL to allow non-IP traffic through.

How Data Moves Through the Transparent Firewall

Figure 4-8 shows a typical transparent firewall implementation with an inside network that contains a public web server. The FWSM has an ACL so that the inside users can access Internet resources. Another ACL allows the outside users to access only the web server on the inside network.

Figure 4-8   Typical Transparent Firewall Data Path

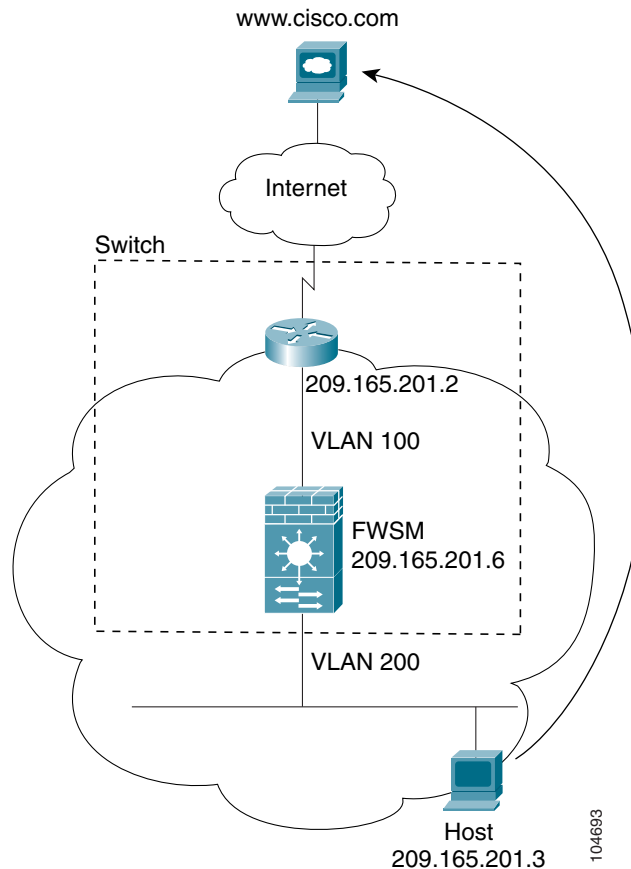The following sections describe how data moves through the FWSM:

- An Inside User Visits a Website, page 4-13
- An Outside User Visits a Website on the Inside Network, page 4-14
- An Outside User Attempts to Access an Inside Host, page 4-15

An Inside User Visits a Website

Figure 4-2 shows an inside user accessing an outside website.

Figure 4-9   Inside to Outside

The steps below describe how data moves through the FWSM (see Figure 4-2):

1. The user on the inside network requests a web page from www.cisco.com.

2. The FWSM receives the packet on VLAN 200 and, because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (ACLs, filters, AAA).

   For multiple context mode, the FWSM first classifies the packet according to either a unique VLAN or a unique destination address. In this case, the VLAN would be unique. For transparent firewall mode, each context has a unique VLAN on the inside and outside, so the IP address would not be considered.

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 on VLAN 100.

   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. When the 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.

6. The FWSM forwards the packet to the inside user.

An Outside User Visits a Website on the Inside Network

Figure 4-3 shows an outside user accessing the inside website.

Figure 4-10   Outside to Inside
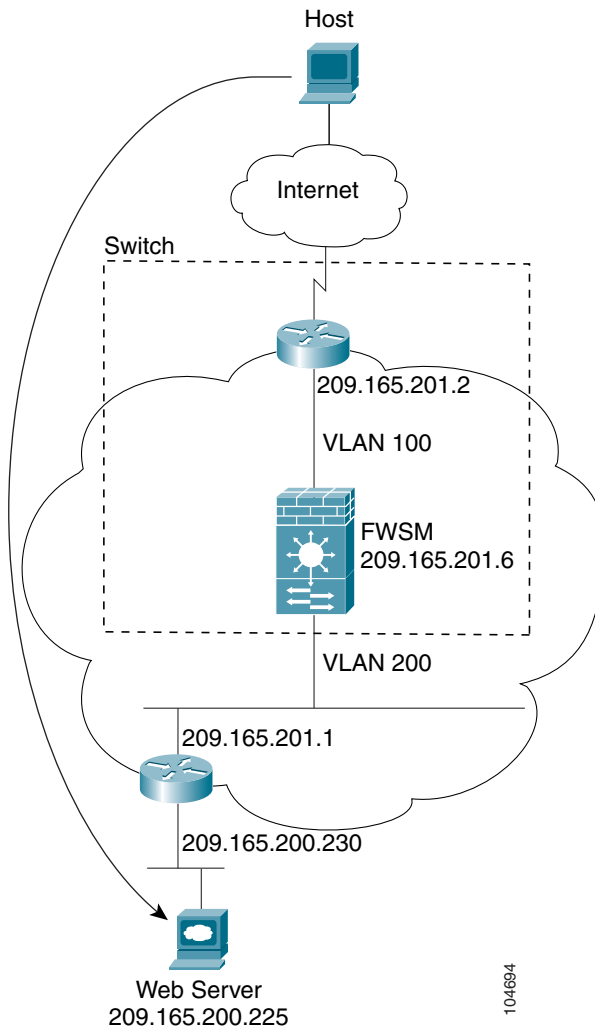
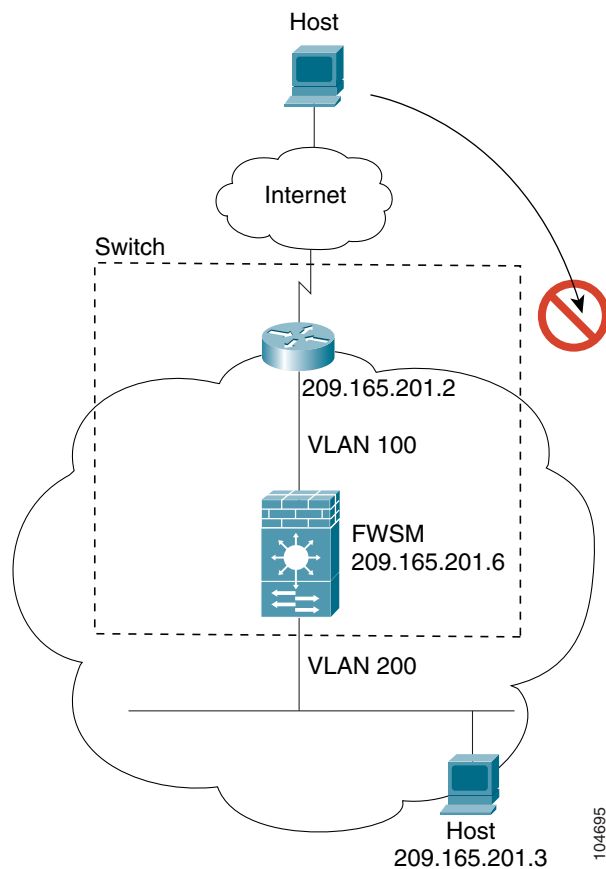The steps below describe how data moves through the FWSM (see Figure 4-3):

1. A user on the outside network requests a web page from the inside website.

2. The FWSM receives the packet on VLAN 100 and, because it is a new session, it verifies that the packet is allowed according to the terms of the security policy (ACLs, filters, AAA).

   For multiple context mode, the FWSM first classifies the packet according to either a unique VLAN or a unique destination address. In this case, the VLAN would be unique. For transparent firewall mode, each context has a unique VLAN on the inside and outside, so the IP address would not be considered.

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 on VLAN 200.

    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. When the website 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.

6. The FWSM forwards the packet to the outside user.

An Outside User Attempts to Access an Inside Host

Figure 4-5 shows an outside user attempting to access a host on the inside network.

Figure 4-11   Outside to Inside

The steps below describe how data moves through the FWSM (see Figure 4-5):

1. A user on the outside network attempts to reach an inside host.

2. The FWSM receives the packet and, because it is a new session, it verifies if the packet is allowed according to the terms of the security policy (ACLs, filters, AAA).

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. See the "Other Protection Features" section on page 1-6 for more information.

Setting the Firewall Mode

You can set the FWSM to run in routed firewall mode (the default) or transparent firewall mode.

For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system configuration.

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. See the "Backing Up the Configuration" section on page 16-7 for more information.

If you download a text configuration to the FWSM that changes the mode with the **firewall transparent** command (see below), 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 the system execution space:

  ```
  FWSM(config)# firewall transparent
  ```

  This command also appears in each context configuration for informational purposes only; you cannot enter this command in a context.

- To set the mode to routed, enter the following command in the system execution space:

  ```
  FWSM(config)# no firewall transparent
  ```