



Introduction to the Firewall Services Module

The FWSM is a high-performance, space-saving, stateful firewall module that installs in the Catalyst 6500 series switches and the Cisco 7600 series routers.

Firewalls protect inside networks from unauthorized access by users on an outside network. The firewall can also protect inside networks from each other, for example, by keeping a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such as a web or FTP server, you can place these resources on a separate network behind the firewall, called a *demilitarized zone* (DMZ). The firewall allows limited access to the DMZ, but because the DMZ includes only the public servers, an attack there affects only the servers and does not affect the other inside networks. You can also control when inside users access outside networks (for example, access to the Internet), by allowing only certain addresses out, by requiring authentication or authorization, or by coordinating with an external URL filtering server.

The FWSM includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, hundreds of interfaces, and many more features.

When discussing networks connected to a firewall, the *outside* network is in front of the firewall, the *inside* network is protected and behind the firewall, and a *DMZ*, while behind the firewall, allows limited access to outside users. Because the FWSM lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

This chapter includes the following sections:

- [Security Policy Overview, page 1-1](#)
- [How the Firewall Services Module Works with the Switch, page 1-3](#)
- [Firewall Mode Overview, page 1-5](#)
- [Stateful Inspection Overview, page 1-6](#)
- [Security Context Overview, page 1-7](#)

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. The FWSM does not allow any traffic to pass through unless explicitly allowed by an access list. You can apply actions to traffic to customize the security policy. This section includes the following topics:

- [Permitting or Denying Traffic with Access Lists, page 1-2](#)

- [Applying NAT, page 1-2](#)
- [Using AAA for Through Traffic, page 1-2](#)
- [Applying Internet Filtering, page 1-2](#)
- [Applying Application Inspection, page 1-2](#)
- [Applying Connection Limits, page 1-3](#)

Permitting or Denying Traffic with Access Lists

You can apply an access list to allow traffic through an interface. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.

Applying NAT

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.

Using AAA for Through Traffic

You can require authentication and/or authorization for certain types of traffic, for example, for HTTP. The FWSM also sends accounting information to a RADIUS or TACACS+ server.

Applying Internet Filtering

Although you can use access lists to prevent outbound access to specific websites or FTP servers, configuring and managing web usage this way is not practical because of the size and dynamic nature of the Internet. We recommend that you use the FWSM in conjunction with a separate server running one of the following Internet filtering products:

- Websense Enterprise
- Sentian by N2H2

Applying Application Inspection

Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the FWSM to do a deep packet inspection.

Applying Connection Limits

You can limit TCP and UDP connections and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. The FWSM uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

How the Firewall Services Module Works with the Switch

You can install the FWSM in the Catalyst 6500 series switches and the Cisco 7600 series routers. The configuration of both series is identical, except for the following variations:

- The Catalyst 6500 series switches supports two software modes:
 - Cisco IOS software on both the switch supervisor and the integrated MSFC (known as “supervisor IOS”).
 - Catalyst Operating System (OS) on the supervisor, and Cisco IOS software on the MSFC.

For commands and configuration that are performed on the switch itself, both modes are described.

- The Cisco 7600 series routers support only Cisco IOS software.

Both series are referred to generically in this guide as the “switch.”

The FWSM runs its own operating system.

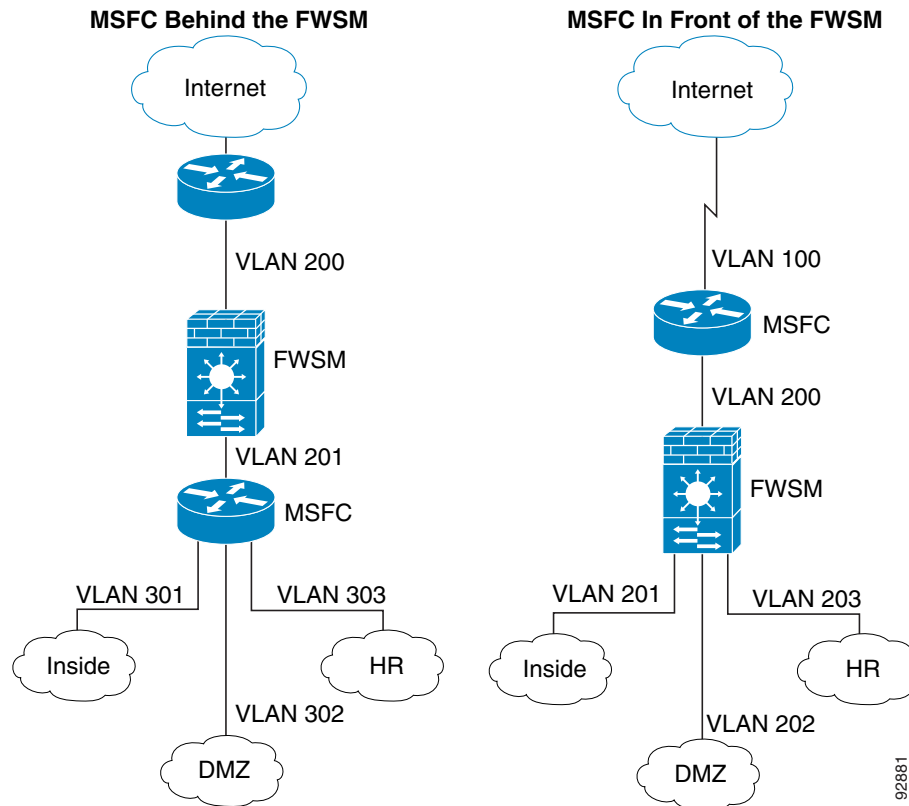
Using the MSFC

The switch includes a switching processor (the supervisor) and a router (the MSFC). Although you need the MSFC as part of your system, you do not have to use it. If you choose to do so, you can assign one or more VLAN interfaces to the MSFC (if your switch software version supports multiple SVIs; see [Table A-1 on page A-2](#)). In single context mode, you can place the MSFC in front of the firewall or behind the firewall (see [Figure 1-1](#)).

The location of the MSFC depends entirely on the VLANs that you assign to it. For example, the MSFC is behind the firewall in the example shown on the left side of [Figure 1-1](#) because you assigned VLAN 201 to the inside interface of the FWSM. The MSFC is in front of the firewall in the example shown on the right side of [Figure 1-1](#) because you assigned VLAN 200 to the outside interface of the FWSM.

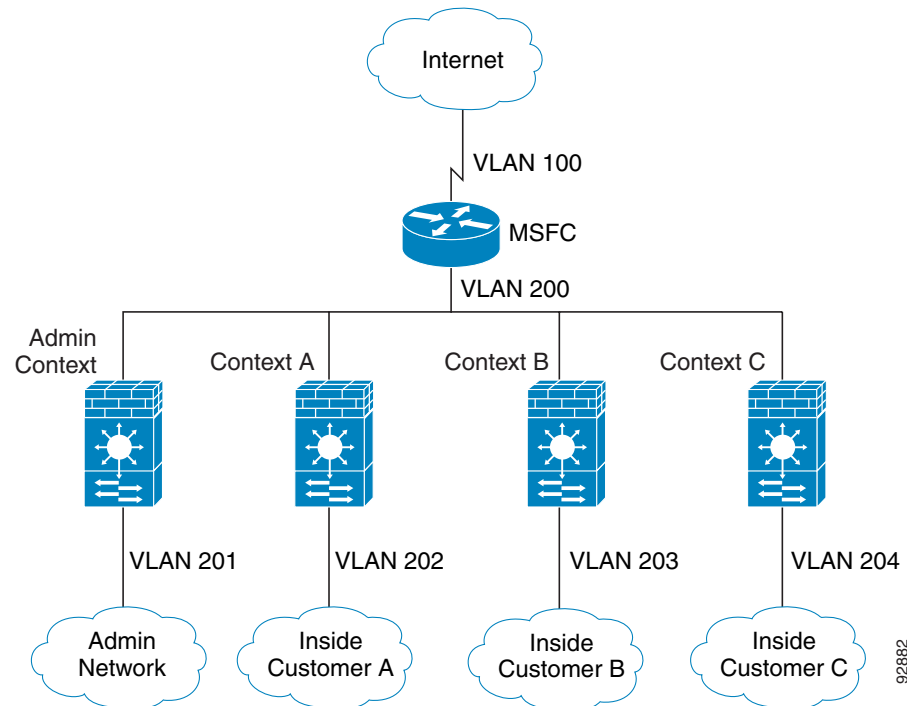
In the left-hand example, the MSFC routes between VLANs 201, 301, 302, and 303, and no inside traffic goes through the FWSM unless it is destined for the Internet. In the right-hand example, the FWSM processes and protects all traffic between the inside VLANs 201, 202, and 203.

Figure 1-1 MSFC Placement



For multiple context mode, if you place the MSFC behind the FWSM, you should only connect it to a single context. If you connect the MSFC to multiple contexts, the MSFC will route between the contexts, which might not be your intention. The typical scenario for multiple contexts is to use the MSFC in front of all the contexts to route between the Internet and the switched networks (see [Figure 1-2](#)).

Figure 1-2 MSFC Placement with Multiple Contexts



Firewall Mode Overview

The FWSM runs in two different firewall modes:

- Routed
- Transparent

In routed mode, the FWSM is considered to be a router hop in the network.

In transparent mode, the FWSM acts like a “bump in the wire,” or a “stealth firewall,” and is not considered a router hop. The FWSM connects to the same network on its inside and outside interfaces. You can configure up to eight pairs of interfaces (called bridge groups) to connect to eight different networks, per context.

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow unsupported routing protocols.

In multiple context mode, you can choose the mode for each context independently, so some contexts can run in transparent mode while others can run in routed mode.

Stateful Inspection Overview

All traffic that goes through the firewall is inspected using the Adaptive Security Algorithm and is either allowed through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process.

A stateful firewall like the FWSM, however, takes into consideration the state of a packet:

- Is this a new connection?

If it is a new connection, the firewall has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the “session management path,” and depending on the type of traffic, it might also pass through the “control plane path.”



Note The first packet for a session cannot be comprised of fragments for a packet that is larger than 8500 Bytes. The session will be established, but only the first 8500 Bytes will be sent out. Subsequent packets for this session are not affected by this limitation.

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the “fast path”

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels: a data channel, which uses well-known port numbers, and a control channel, which uses different port numbers for each session. These protocols include FTP, H.323, and SNMP.



Note The FWSM performs session management path and fast path processing on three specialized networking processors. The control plane path processing is performed in a general-purpose processor that also handles traffic directed to the FWSM and configuration and management tasks.

- Is this an established connection?

If the connection is already established, the firewall does not need to recheck packets; most matching packets can go through the fast path in both directions. The fast path is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions
- Layer 3 and Layer 4 header adjustments

For UDP or other connectionless protocols, the FWSM creates connection state information so that it can also use the fast path.

Data packets for protocols that require Layer 7 inspection can also go through the fast path.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection.

**Note**

For QoS compatibility, the FWSM preserves the DSCP bits for all traffic that passes through the FWSM.

Security Context Overview

You can partition a single FWSM into multiple virtual devices, known as security contexts. Each context has its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, and management. Some features are not supported, including dynamic routing protocols.

In multiple context mode, the FWSM includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the FWSM. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts.

**Note**

Multiple context mode supports static routing only.
