Introduction to the Firewall Services Module

The Firewall Services Module (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 only includes the public servers, an attack there only affects 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.

Note 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.

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.

This chapter contains the following sections:

- Chassis System Requirements, page 1-2
- How the Firewall Services Module Works, page 1-7

Chassis System Requirements

The switch models that support the FWSM include the following platforms:

- Catalyst 6500 series switches, with the following required components:
  - Supervisor engine with Cisco IOS software (known as supervisor IOS) *or* Catalyst operating system (OS). See Table 1-1 for supported supervisor engine and software releases.
  - Multilayer Switch Feature Card (MSFC 2) with Cisco IOS software. See Table 1-1 for supported Cisco IOS releases.
- Cisco 7600 series routers, with the following required components:
  - Supervisor engine with Cisco IOS software. See Table 1-1 for supported supervisor engine and software releases.
  - MSFC 2 with Cisco IOS software. See Table 1-1 for supported Cisco IOS releases.

Note The FWSM does not support a direct connection to a switch WAN port because WAN ports do not use static virtual local area networks (VLANs). However, the WAN port can connect to the MSFC, which can connect to the FWSM.

Table 1-1 shows the supervisor engine version, software, and supported FWSM features.

Table 1-1 Support for FWSM 2.2 Features

		FWSM Features:	
	Supervisor Engines[1]	**Multiple SVIs**[2]	**Transparent Firewall with Failover**[3]
Cisco IOS			
12.1(13)E	2	No	No
12.1(19)E	2	**Yes**	No
12.1(22)E and higher	2	**Yes**	**Yes**
12.2(14)SY and higher	2	**Yes**	No
12.2(14)SX	2, 720	No	No
12.2(17a)SX3	2, 720	**Yes**	**Yes**
12.2(17b)SXA	2, 720	**Yes**	**Yes**
12.2(17d)SXB and higher	2, 720	**Yes**	**Yes**
Catalyst OS[4]			
7.5(x)	2	No	No
7.6(1) through 7.6(4)	2	**Yes**	No
7.6(5) and higher	2	**Yes**	**Yes**
8.2(x)	2, 720	**Yes**	**Yes**
8.3(x)	2, 720	**Yes**	**Yes**

[1] The FWSM does not support the supervisor 1 or 1A.

[2] Supports multiple switched VLAN interfaces (SVIs) between the MSFC and FWSM. An SVI is a VLAN interface that is routed on the MSFC.

[3] Supports transparent firewall mode when you use failover. Failover requires BPDU forwarding to the FWSM, or else you can have a loop. Other releases that do not support BPDU forwarding only support transparent mode without failover.

[4] When you use Catalyst OS on the supervisor, you can use any of the supported Cisco IOS releases above on the MSFC. (When you use Cisco IOS software on the supervisor, you use the same release on the MSFC.) The supervisor software determines the FWSM feature support. For example, if you use Catalyst OS Release 7.6(1) on the supervisor and Cisco IOS 12.1(13)E on the MSFC, then the switch does support multiple SVIs, because Catalyst OS Release 7.6(1) supports multiple SVIs.

Features

This section describes the FWSM features, and includes the following topics:

- Features, page 1-3
- Stateful Inspection Feature, page 1-5
- Other Protection Features, page 1-6

General Features

Table 1-2 lists the features of the FWSM.

Table 1-2 General FWSM Features

Feature	Description
Transparent firewall or routed firewall mode	The firewall can run in one of the following modes: • Routed—The FWSM is considered to be a router hop in the network. It performs NAT[1] between connected networks. In single context mode, you can use OSPF[2] or passive RIP[3]. • Transparent—The FWSM acts like a "bump in the wire," 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.
Multiple security contexts	In multiple context mode, you can create up to 100 separate security contexts (depending on your software license). A security context is a virtual firewall that has its own security policy and interfaces. Multiple contexts are similar to having multiple stand-alone firewalls. Contexts are conveniently contained within a single module. You can run all security contexts in routed mode or in transparent mode; you cannot run some contexts in one mode and others in another. With the default software license, you can run up to two security contexts in addition to an admin context. For more contexts, you must purchase a license.
Resource management for security contexts	You can limit resources per context so one context does not use up too many resources. You create classes that define resource limitations as an absolute value or as a percentage, and then assign a context to one of these classes.
Communication between same security level	You can configure interfaces on the same security level to communicate with each other. This feature is off by default, and you can enable or disable this feature on a per context basis. In earlier releases, no communication between interfaces with the same security level was possible.
Bidirectional NAT and policy NAT	You can perform NAT on inside and outside addresses. For policy NAT, you can identify addresses to be translated using an extended ACL[4], which allows you more control in determining which addresses to translate.

Table 1-2 General FWSM Features (continued)

Feature	Description
Several ACL types	The FWSM supports the following ACLs: • Extended ACL to control IP traffic on an interface: – Inbound – Outbound • For transparent firewall mode, EtherType ACL to control non-IP traffic on an interface: – Inbound – Outbound • Standard ACL for OSPF route redistribution.
URL Filtering	Filter HTTP, HTTPS, and FTP requests using Websense Enterprise or Sentian by N2H2.
Dynamic Routing Protocols	Single context mode only. • RIP v1 and v2 (passive mode) • OSPF **Note** Multiple context mode supports static routing only.
DHCP server and DHCP relay	The FWSM acts as a DHCP[5] server. The FWSM also supports DHCP relay to forward DHCP requests to an upstream router.
Management	The FWSM supports the following management methods: • Cisco PDM for FWSM—Release 4.0 supports FWSM Release 2.2 features. PDM is a browser-based configuration tool that resides on the FWSM. The system administrator can configure multiple security contexts. If desired, individual context administrators can configure only their contexts. • Cisco Firewall MC[6]—Release 1.3.1 supports FWSM Release 2.2 features. For multiple context mode, Release 1.3.1 supports management of each context separately but does not support system-level operations, such as adding or deleting contexts, or the provisioning of failover in multiple mode. • CLI[7]
Login banners	You can define a text message to display when users log into the FWSM.
System message enhancements	You can configure ACLs to generate system messages when they match traffic. You can also set the level for a system message.

[1] Network Address Translation
[2] Open Shortest Path First
[3] Routing Information Protocol
[4] access control lists
[5] Dynamic Host Configuration Protocol
[6] Firewall Management Center
[7] command-line interface

Stateful Inspection Feature

All traffic that goes through the firewall is inspected using the Adaptive Security Algorithm (ASA) and 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 ACLs 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."

  The session management path is responsible for the following tasks:

  - Performing the ACL 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 (NPs). 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 re-check 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

  The following types of traffic go through the fast path:

  - Established TCP or UDP connections

    For UDP, which does not have sessions, the FWSM creates UDP connection state information so that it can also use the fast path.

  - ICMP control packets
  - Data packets for protocols that require Layer 7 inspection

  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.

Other Protection Features

Table 1-3 describes the protection features provided by the FWSM. These features control network activity associated with specific kinds of attacks.

Table 1-3 Protection Features

Protection Feature	Description
ARP Inspection	For transparent firewall mode, you can enable ARP inspection. By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the FWSM. When you enable ARP inspection, the FWSM compares the MAC address and IP address in all ARP packets to static entries in the ARP table. Enable this feature using the **arp inspection** command.
DNS Guard	DNS Guard identifies each outbound DNS[1] resolve request, and allows only a single DNS response. A host might query several servers for a response (in the case that the first server is slow in responding), but only the first answer to the request is allowed. All additional responses to the request are dropped by the firewall. This feature is always enabled. This feature is unrelated to the DNS inspection engine.
Flood Guard	Flood Guard controls the tolerance of the AAA server for unanswered login attempts. This helps to prevent a DoS[2] attack on AAA services in particular. This feature optimizes AAA system use. Flood Guard is enabled by default and can be controlled with the **floodguard** command.
Frag Guard	Frag Guard provides IP fragment protection, and can be configured with the **fragment** command. **Note** In FWSM 1.1, the default fragment size was 1, which caused the FWSM to drop all fragments by default. In FWSM 2.2, the default fragment size is 200 (the same as the PIX default).
ICMP Filtering	The FWSM automatically denies ICMP access to FWSM interfaces. This feature shields FWSM interfaces from detection by users on an external network. You can allow ICMP to FWSM interfaces using the **icmp** command.
Mail Guard	Mail Guard provides safe access for SMTP[3] connections from the outside to an inside messaging server. This feature lets you deploy a single mail server within the internal network without it being exposed to known security problems with some SMTP server implementations. This eliminates the need for an external mail relay (or bastion host) system. Mail Guard enforces a safe minimal set of SMTP commands to avoid an SMTP server system from being compromised. Enable this feature using the **fixup protocol smtp 25** command.
TCP Intercept	TCP Intercept protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN[4] packets. Enable this feature by setting the maximum embryonic connections option of the **nat** and **static** commands. When the embryonic limit has been surpassed, the TCP intercept feature intercepts TCP SYN packets from clients to servers on a higher security level. The software establishes a connection with the client on behalf of the destination server and, if successful, establishes the connection with the server on behalf of the client, then combines the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. **Note** The PIX firewall accomplishes TCP intercept functionality using SYN cookies; the FWSM uses a different method, but accomplishes the same goal.
Unicast Reverse Path Forwarding	Unicast RPF helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. Enable this feature using the **ip verify reverse-path** command.

[1] Domain Name System

[2] denial of service

[3] Simple Mail Transfer Protocol

[4] synchronization

How the Firewall Services Module Works

This section describes the network firewall functionality provided by the FWSM. It includes the following topics:

Security Policy Overview

A security policy determines which traffic is allowed to pass through the firewall to access another network. By default, no traffic can pass through the firewall. By applying ACLs to interfaces, you can determine which IP addresses and traffic types can pass through the interfaces to access other networks.

Note By default, the Cisco PIX firewall allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). However, the FWSM does not allow *any* traffic to pass between interfaces unless you explicitly permit it with an ACL. This rule is true for both routed firewall mode and transparent firewall mode. While you still specify the security level for an interface on the FWSM, the security level does not provide explicit permission for traffic to travel from a high security interface to a low security interface. See the "Configuring Interfaces" section on page 6-6 for more information about how security levels work.

For routed firewall mode, in addition to ACLs, you can use Network Address Translation (NAT) between networks to further protect the real IP addresses of hosts.

If you have an AAA server, you can also apply AAA rules to users to control their access.

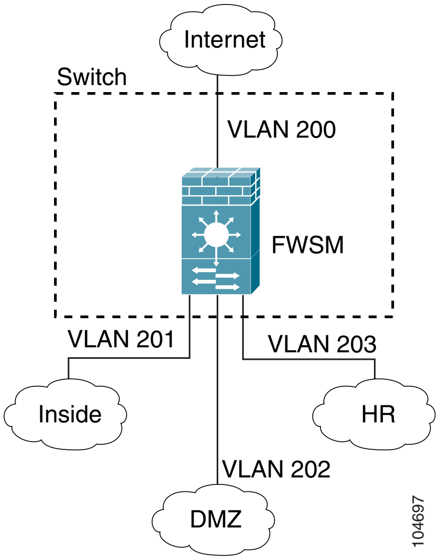
All of these features plus others, such as filters or inspection engines, make up the security policy of the firewall.

VLAN Interfaces

The FWSM does not include any external physical interfaces. Instead, it uses internal VLAN interfaces. For example, you assign VLAN 201 to the FWSM inside interface, and VLAN 200 to the outside interface. You assign these VLANs to physical switch ports, and hosts connect to those ports. When communication occurs between VLANs 201 and 200, the FWSM is the only available path between the VLANs, forcing traffic to be statefully inspected.

Figure 1-1 shows the FWSM with 4 interfaces: one outside interface (VLAN 200), one DMZ interface (VLAN 202), and two inside interfaces (VLAN 201 and 203).

Figure 1-1 VLAN Interfaces



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, based on the PIX operating system. Although the PIX OS is similar to the FWSM OS, there are a number of differences. Many of the differences are enhancements that take advantage of the FWSM hardware and architecture.

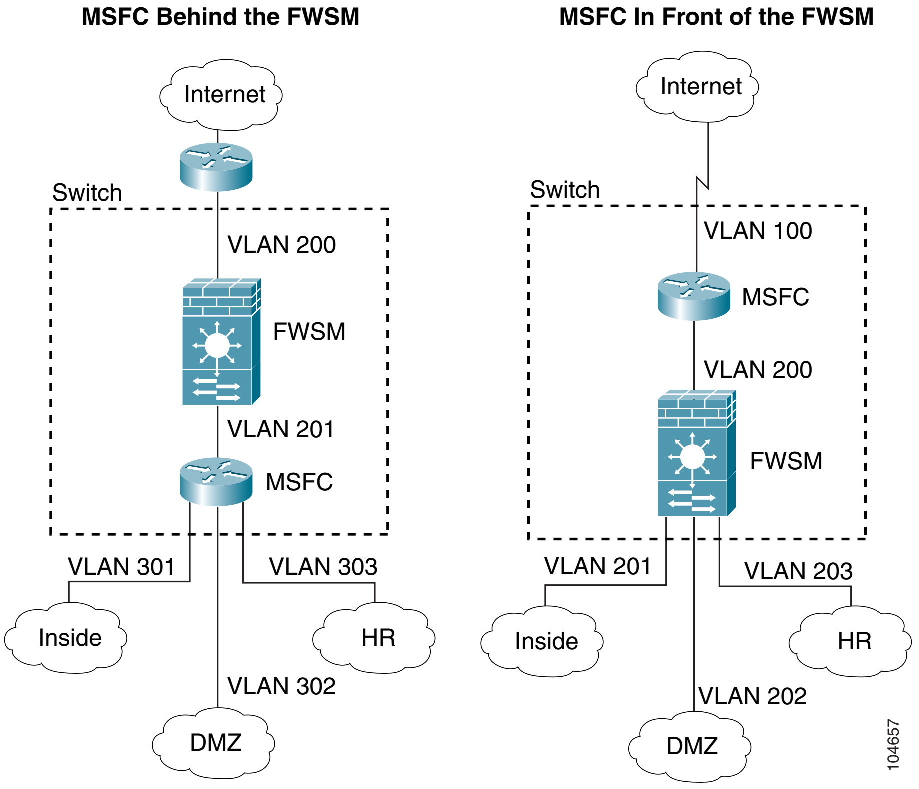
Using the MSFC

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 1-1 on page 1-2). In single context mode, you can place the MSFC in front of the firewall or behind the firewall (see Figure 1-2).

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 1-2 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 1-2 because you assigned VLAN 200 to the outside interface of the FWSM.

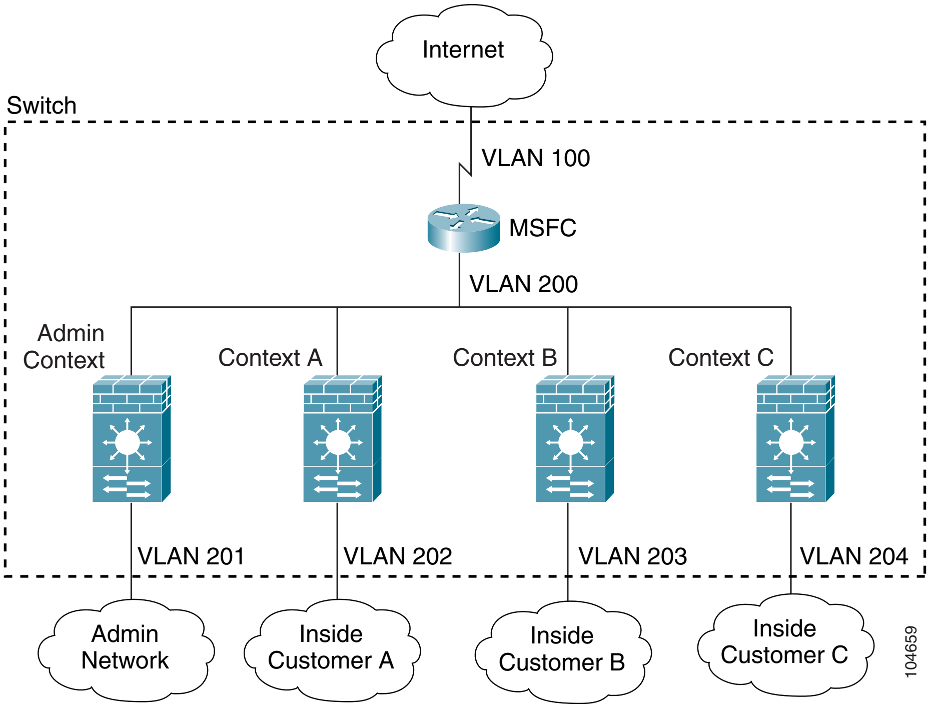
In the left-hand example, the MSFC routes between VLANs 201, 301, 302, and 303, and no inside traffic goes through the FWSM unless it is destined for the Internet. In the right-hand example, the FWSM processes and protects all traffic between the inside VLANs 201, 202, and 203.

Figure 1-2 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 1-3).

Figure 1-3 MSFC Placement with Multiple Contexts



Routed Firewall and Transparent Firewall Modes

The FWSM can run in two firewall modes:

- Routed
- Transparent

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.

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 traffic through. 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.

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 multicast streams using an EtherType ACL.

See Chapter 7, "Configuring Bridging Parameters and ARP Inspection," for more information.

Security Contexts

You can partition a single FWSM into multiple virtual firewalls, known as security contexts. Each context is an independent system, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple stand-alone firewalls.

Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone firewall. If desired, you can allow individual context administrators to implement the security policy on the context. Some resources are controlled by the overall system administrator, such as VLANs and system resources, so that one context cannot affect other contexts inadvertently.

The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the module. The system administrator has privileges to manage all contexts. 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 into the admin context (for example, over an SSH connection), then that user has system administrator rights, and can access the system configuration and all other context configurations. Typically, the admin context provides network access to network-wide resources, such as a syslog server or context configuration server.

With the default software license, you can run up to two security contexts plus the admin context. For more contexts, you must purchase a license.

Note You can run all your contexts in routed mode or transparent mode; you cannot run some contexts in one mode and others in another.

Note Multiple context mode supports static routing only.

See Chapter 5, "Managing Security Contexts," for more information.