



# Overview

---

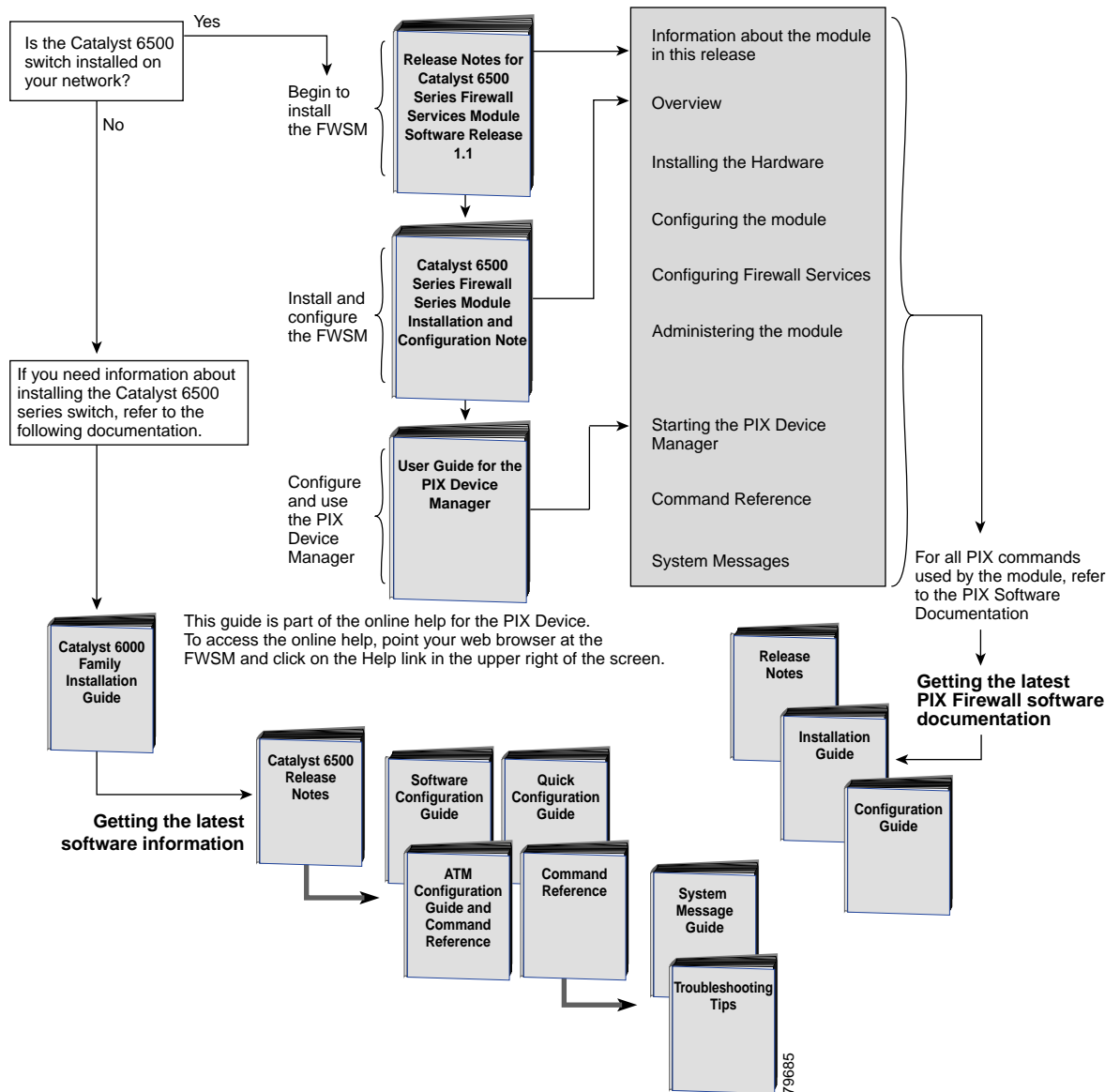
This chapter describes the Catalyst 6500 Series Firewall Services Module, how it operates, and how to manage it. This chapter contains these sections:

- [Before You Begin, page 1-2](#)
- [Understanding How the Firewall Services Module Works, page 1-3](#)
- [Feature Set, page 1-8](#)
- [Specifications and System Limitations, page 1-9](#)
- [Front Panel Description, page 1-11](#)
- [Hardware Specifications, page 1-12](#)

# Before You Begin

To help you get started using the Firewall Services Module, refer to this roadmap:

## Getting Started with the Firewall Services Module



### Note

The Firewall Services Module uses many of the same commands as the PIX application software.

[Table A-1](#) lists the PIX commands used by the module.

[Table A-2](#) lists the Cisco IOS commands for the module.

[Table A-4](#) lists the new commands specific to the module. These commands are described in [Appendix B, “Command Reference.”](#)

[Table A-5](#) lists the PIX commands that were changed for the module.

[Table A-6](#) lists the PIX commands that are not used by the module.

[Table A-7](#) lists the PIX commands used by the module and their PIX version.

# Understanding How the Firewall Services Module Works

Firewalls protect an internal (inside) network, such as a data center, from unauthorized access by users on an external (outside) network, such as the public Internet.

**Note**

The term *inside* refers to networks or network resources protected by the firewall. The term *outside* refers to networks not protected by the firewall.

You also can protect one or more networks, known as *demilitarized zones (DMZs)*. DMZs are those portions of the network that contain resources that you may want to allow access to for specified users. Access to a DMZ is usually more restricted than access to the outside network, but less restricted than access to the inside network.

A DMZ allows you to protect your network resources that need to be accessed by users on the public Internet, for example, mail servers or web servers. By placing them in a DMZ, you obtain some protection without jeopardizing the resources on your internal network.

Connections between the inside and outside and DMZ networks are controlled by the module through the firewall using a network-modeled protection scheme based upon a configuration and security policy. By implementing a security policy, you can ensure that all traffic from the protected networks only passes through the firewall to the unprotected network. You also can control who accesses the networks and with which services. Features on the module allow you to control how your security policy is used.

The security policy determines the security level, which allows you to isolate networks that are assigned the same security level from each other. To route traffic between different networks, you assign each network a different security level. A lower security level provides less protection for the interface than a higher security level. The security levels to your networks can range from 0 to 100.

All interfaces connecting the inside, outside, and DMZ networks through the module are virtual and logical Layer 3 interfaces consisting of a VLAN, an IP address, and a security level. The module supports 100 firewall interfaces. All traffic between these VLANs is protected and controlled. Because the module supports multiple interfaces, you can create one or more DMZ networks.

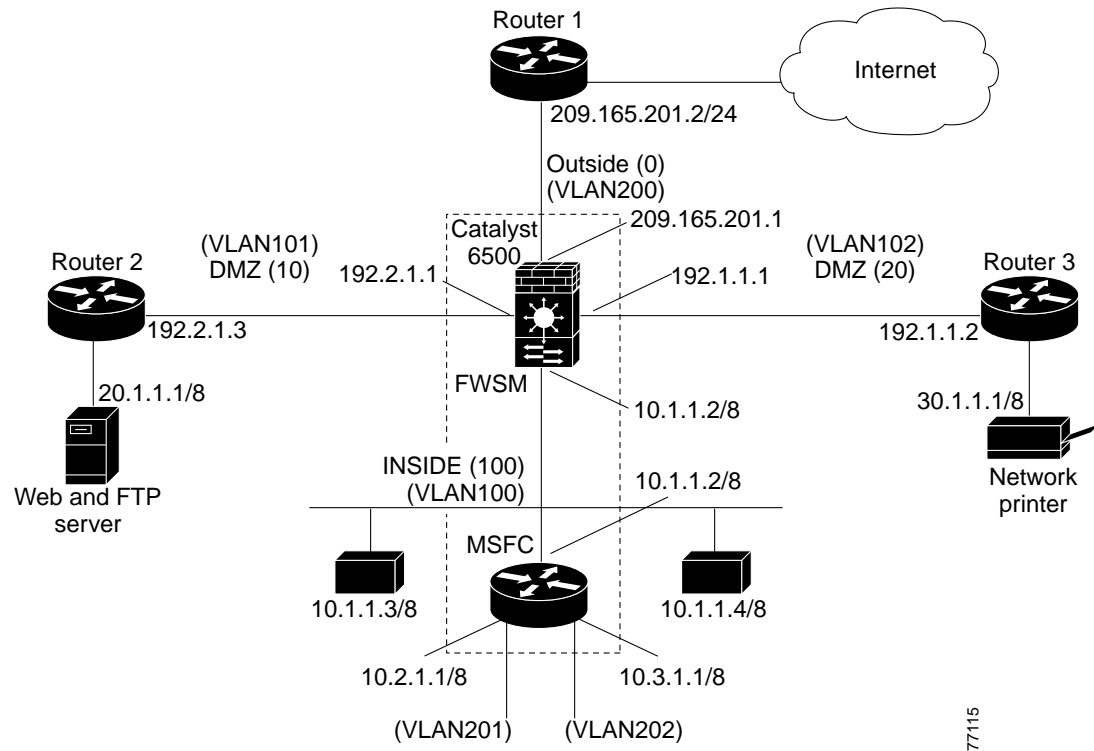
The Firewall Services Module is a fabric-enabled module that connects to both the Catalyst 6500 bus and the Switch Fabric Module if one is present. A Switch Fabric Module is not required for the Firewall Services Module to function.

The module has a 6-Gbps dot1q EtherChannel connection to the backplane where the hosts of the various security zones are connected to ports on the Catalyst 6500 chassis.

The module can be configured in a multiple, failover, or redundant configuration.

[Figure 1-1](#) shows a firewall configuration. The Multilayer Switch Feature Card (MSFC) is used as a router on the network inside the firewall. The MSFC is connected to only one of the controlled firewall interfaces. All other router interfaces configured on the MSFC are considered to be the same security level as the interface to which the MSFC is connected. For example, traffic between VLAN 201 and VLAN 202 is routed directly.

Figure 1-1 Firewall Services Module Configuration



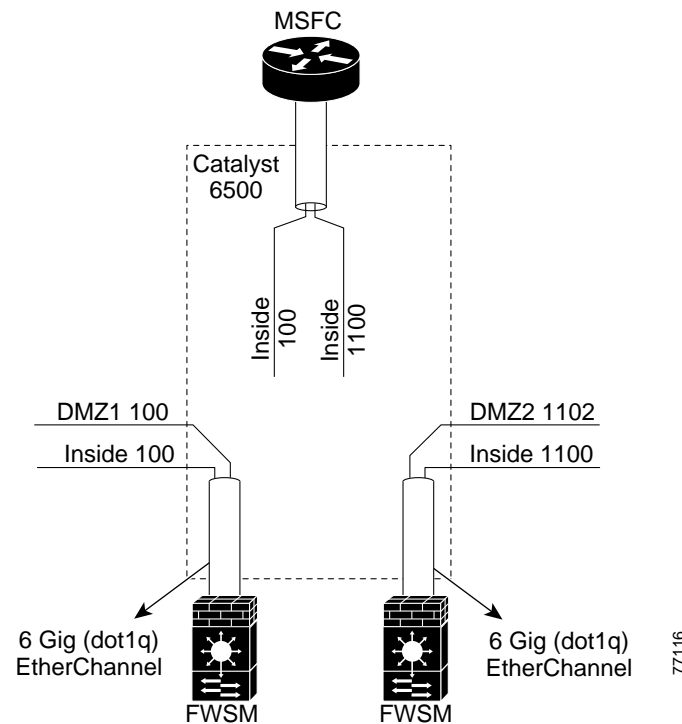
These sections describe firewall configuration and failover:

- [Multiple Firewall Services Module Configuration, page 1-5](#)
- [Redundancy Failover, page 1-5](#)

## Multiple Firewall Services Module Configuration

Figure 1-2 shows multiple modules that are located in the same switch, and how they can operate independently. You can have up to four FWSMs installed in the same switch. The network requirements and topology determine the configuration.

Figure 1-2 Multiple Firewall Services Module Configuration



In a multiple-module configuration, the following conditions apply:

- Modules cannot share the same firewall interface definition. Separate VLANs must be defined for each module.
- Multiple modules in the same chassis do not share loads or synchronize states among each other unless they are configured as active or standby modules.
- Two modules in the same chassis or two modules that are in separate chassis can be configured to maintain firewall protection in case either module fails. When one module (active) fails, another (standby) immediately takes its place.

## Redundancy Failover

The failover configuration has these features:

- A dedicated logical interface is created for failover communication. No failover cable is required in this configuration as is required in the PIX configuration.

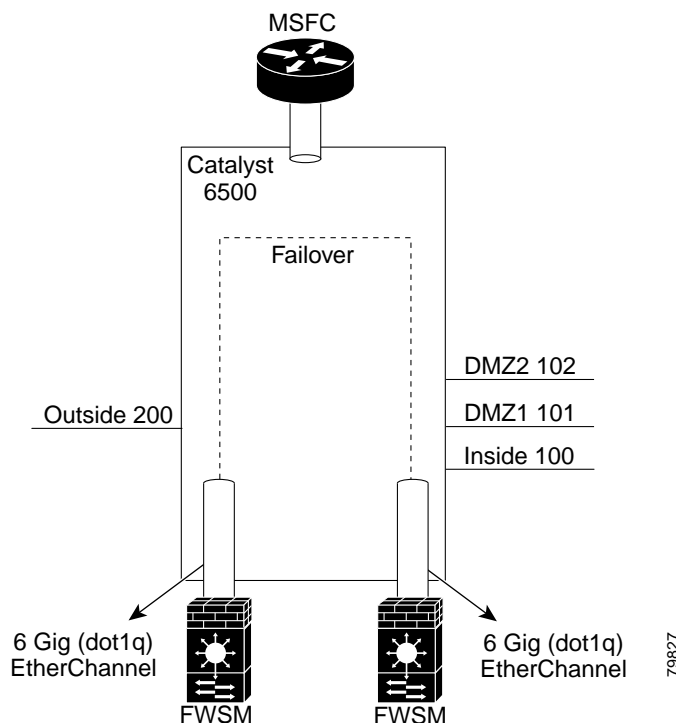


**Note** You must add the dedicated logical VLAN to the VLAN group using the **firewall vlan-group** command and activate the dedicated VLAN using the **VLAN [X] state active** command.

- All firewall interfaces between the active module and standby module are separated from each other in Layer 2. The interfaces on the active module must be present on the standby module and the trunk must be configured to pass all VLANs.
- Both the active module and the standby module have corresponding interfaces in the same VLAN.
- When the active module fails, the switchover to the standby module is transparent to other nodes in the network. After switchover, all interfaces on the new active module have the IP addresses and the MAC addresses of the interfaces of the failed module.

The module can be configured to use stateful failover as shown in [Figure 1-3](#). Stateful failover allows you to maintain the operating state for the connection during the failover from the primary module to the standby module.

**Figure 1-3 Stateful Failover Configuration**



When a failover occurs, each module changes its state. The new active module begins accepting traffic. The new standby module assumes the failover IP and MAC addresses of the module that was previously the active module. Because network devices do not detect a change in these addresses, there are no ARP entries changed nor is there a time out anywhere on the network.

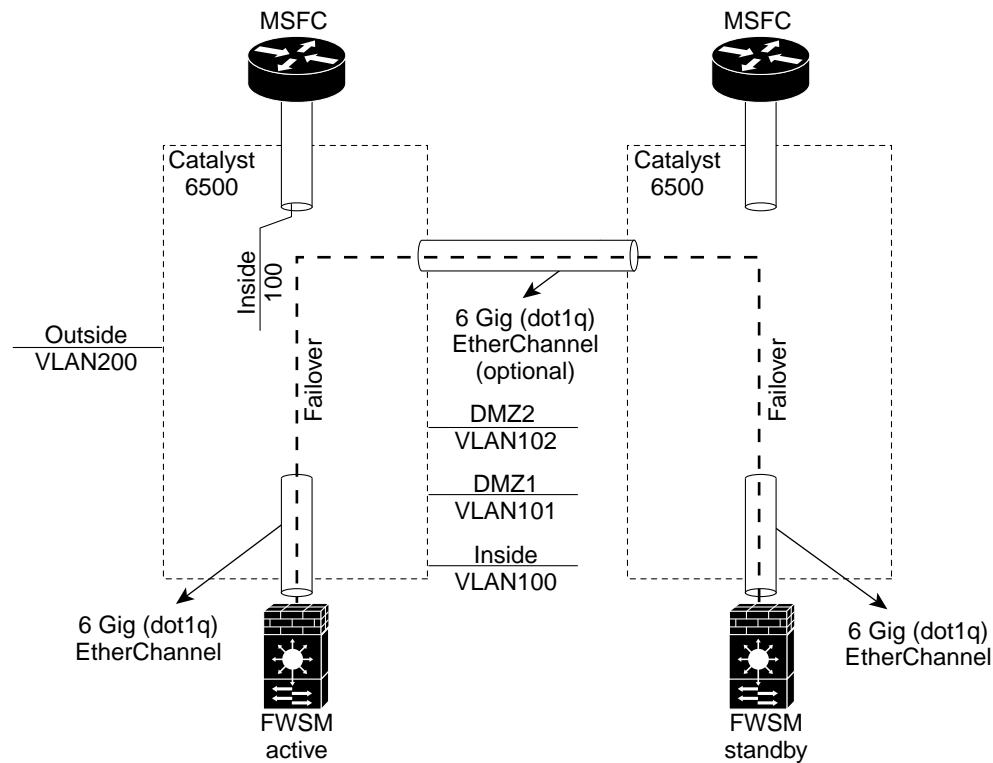
Be sure that both modules have the same software version, VLAN configuration, Flash memory, and RAM; if not, the configuration copied to the standby module will not work. After you configure the primary module and provide the failover link, the primary module automatically copies the configuration over to the standby module.

**Note**

We recommend that you separate the failover and logical update interfaces into separate links. Packets on the failover link are tagged with a higher priority for QOS. Because stateful traffic can be high in volume, the advantages of prioritizing failover traffic are lost by keeping both the failover link and failover LAN interfaces the same.

Figure 1-4 shows two modules located in separate chassis: one module is designated as the active module and the other module is designated as the standby module.

**Figure 1-4 Multiple-Module Configuration in a Network**



77118

In this multiple-module configuration, the following conditions apply:

- A dedicated logical interface is created for failover communication. No failover cable is required in this configuration as is required in the PIX configuration.
- All firewall interfaces between the active module and the standby module are separated from each other by Layer 2 requiring at least a 1-Gigabit link between them. Performance is limited to the link throughput. For better performance, we recommend that you provide up to a 6-Gigabit IEEE 802.1q EtherChannel link.
- Both of the switches have an identical definition of the firewall interfaces on the MSFC.
- There is a dedicated failover interface between the active module and the standby module used for the stateful failover. This interface synchronizes the states between the active module and the standby module.

# Feature Set

The Firewall Services Module (FWSM) is a high performance firewall used on the Catalyst 6500 series switch and Cisco 7600 series router. The FWSM can occupy a single slot in the Catalyst 6500 series and Cisco 7600 series chassis or two slots in a redundant configuration. Two modules can also reside in separate chassis in a failover configuration.

The Firewall Services Module provides the following features:

- Switch fabric compatibility.
- Interface configuration that can be done through both the native Cisco IOS command-line interface and the module command-line interface.
- PIX 6.0-based feature set and some 6.2 features.
- LAN failover active or standby (both intra- or inter-chassis).
- Dynamic routing, Open Shortest Path First protocol (OSPF) (the module maintains its own OSPF tables), and Routing Information Protocol (RIP).
- IPSec for management only.
- Command authorization.
- Object grouping.
- URL filtering enhancement—The module checks the outgoing URL requests with the policy defined on a Websense, Windows NT, or UNIX-based server. The module either permits or denies the connection depending on the response from the server, which matches a request against a list of website characteristics that are considered inappropriate for business use.
- Support for PIX 6.0 application inspection which ensures the secure use of applications and services. Application inspection rules are configured using the **fixup** command, which is why application inspection is called “fixup.”




---

**Note** Throughout this document, the term “fixup” applies to application inspection and configuring the application inspection process or application inspection rules.

---

- Support for Lightweight Directory Access Protocol (LDAP) or Input [buffer] Limiting Scheme (ILS) fixup for NetMeeting.
- Security—Cisco firewalls provide the latest in security technology, ranging from stateful inspection firewalls to content-filtering capabilities that help protect your network environment from future attacks. Another security feature is the Adaptive Security Algorithm (ASA), which maintains the firewalled areas between the networks controlled by the firewall.

The stateful, connection-oriented ASA creates session flows based on source and destination addresses, TCP sequence numbers (which are non-predictable), port numbers, and additional TCP flags. You can control all inbound and outbound traffic by applying security policies to each connection table entry.

- Reliability—Cisco firewalls provide adaptable security services for operation-critical network environments by using the integrated stateful failover capabilities within the module. Network traffic can be sent automatically to a hot standby module in the event of a failure, while maintaining concurrent connections with automated state synchronization between the primary module and the standby module.

- Network Address Translation (NAT) and Port Address Translation (PAT)—Cisco firewalls provide NAT and PAT services that conceal IP addresses of internal networks and expand network address space for internal networks.
- Denial-of-service (DoS) attack prevention—Cisco firewalls protect the firewall and networks behind them from attempts to gain access, which can bring a network to a halt.
- Cisco PIX Device Manager (PDM) 2.1 support—PDM is a browser-based Java applet you can use to configure the Firewall Services Module.
  - PDM must be downloaded and installed for the Firewall Services Module release 1.1. Refer to the “[Upgrading the PDM](#)” section on page 3-10 of the *Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module Installation and Configuration Note* for download and installation information.
  - The Firewall Services Module 1.1(2) software release is shipped with a preinstalled PDM 2.1 image. You can download the image from CCO to upgrade PDM if necessary.

When the Firewall Services Module software is the platform, PDM will display modified screens for features not supported by the module. To use the PDM to configure the module, refer to the *Cisco PIX Device Manager Installation Guide*, Version 2.1.

The following PIX firewall features are not supported by the module:

- Virtual private networks (VPN) (The module supports IPSec VPN only for management purposes.)
- Intrusion detection system (IDS) syslog messages.
- Cisco Secure Policy Manager (CSPM)
- Conduits
- DHCP (Dynamic Host Configuration Protocol) client

## Specifications and System Limitations

Table 1 lists the specifications and system limitations of the FWSM.

**Table 1** FWSM Specifications and System Limitations

Specification Type	Specification Names	Description
Physical Attributes	Modules per switch	Maximum of four modules per switch. If you are using failover, you can still only have four modules per switch even if two of them are in standby mode.
	Memory	<ul style="list-style-type: none"> <li>• 1 GB RAM.</li> <li>• 128 MB Flash memory.</li> </ul>
	Bandwidth	CEF256 line card with a 6-Gbps path to the Switch Fabric Module (if present) or the 32-Gbps shared bus.
Feature Limits	Filtering servers	16 Websense Enterprise filtering servers.
Managed System Resources	IPSec management connections, concurrent	5 connections.

Table 1 FWSM Specifications and System Limitations (continued)

Specification Type	Specification Names	Description
	TCP <sup>1</sup> or UDP <sup>2</sup> connections between any two hosts, including connections between one host and multiple other hosts, concurrent and rate	999,900 connections. 100K connections per second.
	Fixup connections, rate	10,000 per second.
	PC based fixup connections, rate	10K per second.
	Host connections, concurrent	256K
	SSH <sup>3</sup> management connections, concurrent	5 connections.
	System messages, rate	20K per second.
	Telnet management connections, concurrent	5 connections.
	NAT translations, concurrent	256K.
<b>Fixed System Resources</b>	NAT statements	1K statements.
	High-performance firewall	5 GBps (aggregated).
	Concurrent connections.	1 million
	Packets-per-second.	3 million pps
	New connections per second for HTTP, DNS, and enhanced Simple Mail Transfer Protocol (SMTP).	7K
	VLAN interfaces (no physical interfaces on the module).	100
	Static NAT statements	1K statements.
	Global statements	1K statements.
	Shun statements	2K statements. The FWSM supports at most 2000 shuns - that number is contingent upon finite hardware resources and cannot be increased.
	Alias statements	1K statements.
	User authentication sessions, concurrent	5K sessions.
	User authorization sessions, concurrent	150K sessions. Maximum 15 sessions per user.
	ARP <sup>4</sup> table entries, concurrent	64K entries.
	Route table entries, concurrent	32K entries.
	Packet reassembly, concurrent	30,000 fragments.
<b>Rules</b>	Filter Rules, Fixup and Filter statements combined.	3K rules and statements.

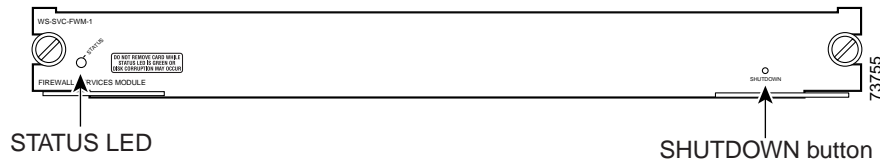
**Table 1** FWSM Specifications and System Limitations (continued)

Specification Type	Specification Names	Description
	Established CLI Rules	1K rules.
	Established data	1K implicit rules used by TCP and UDP fixups to allow back channels.
		3K statements.
	AAA Rules	3K rules. 1K rules for authentication, 1K rules for authorization, and 1K rules for accounting.
	ICMP <sup>5</sup> , Telnet, SSH, and HTTP <sup>6</sup> Rules	1K rules.
	ACEs	72K ACEs (best case).

1. Transmission Control Protocol
2. User Datagram Protocol
3. Secure Shell
4. Address Resolution Protocol
5. Internet Control Message Protocol
6. HyperText Transfer Protocol

## Front Panel Description

The front panel includes a STATUS LED and SHUTDOWN button. (See [Figure 1-5](#))

**Figure 1-5** Firewall Services Module Front Panel

These sections describe the front panel components:

- [STATUS LED](#), page 1-11
- [SHUTDOWN Button](#), page 1-12

## STATUS LED

The STATUS LED indicates the operating states of the module. [Table 1-2](#) describes the LED operation.

**Table 1-2** STATUS LED Description

Color	Description
Green	All diagnostic tests pass. The module is operational.
Red	A diagnostic other than an individual port test failed.

**Table 1-2** STATUS LED Description (continued)

Color	Description
Orange	Indicates one of three conditions: <ul style="list-style-type: none"> <li>• The module is running through its boot and self-test diagnostic sequence.</li> <li>• The module is disabled.</li> <li>• The module is in the shutdown state.</li> </ul>
Off	The module power is off.

## SHUTDOWN Button



### Caution

Do not remove the module from the switch until the module has shut down completely and the STATUS LED is orange or off. You can damage the module if you remove it from the switch before it completely shuts down.

To avoid corrupting the compact Flash memory, you must correctly shut down the module before you remove it from the chassis or disconnect the power. This shutdown procedure is initiated normally by commands entered at the supervisor engine CLI prompt or the module CLI prompt.

If the module fails to respond to these commands properly, you must use the SHUTDOWN button on the front panel to initiate the shutdown procedure. Use a small pointed object (such as a paper clip) to push the button.

The shutdown procedure may require several minutes. The STATUS LED turns orange when the module shuts down.

## Hardware Specifications

Table 1-3 describes the specifications for the module.

**Table 1-3** Specifications

Specification	Description
Dimensions (H x W x D)	1.18 x 15.51 x 16.34 in. (30 x 394 x 415 mm)
Weight	Minimum: 3 lb (1.36 kg) Maximum: 5 lb (2.27 kg)
Environmental conditions:	
Operating temperature	32 to 104°F (0 to 40°C)
Nonoperating temperature	-40 to 167°F (-40 to 75°C)
Humidity	10 to 90%, noncondensing