



CHAPTER 7

Firewall Services Module

This chapter describes the Firewall Services Module (WS-SVC-FWM-1-K9).

The Firewall Services Module protects an internal (inside) network from unauthorized access by users on an external (outside) network, such as the public Internet.



Note

Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.



Note

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

The Firewall Services Module has the following features:

- Multiple modules—Supports multiple Firewall Services Modules in a Cisco 7600 series routers chassis.
- Switch fabric-compatible.
- Interface configuration—Performed though native IOS CLI.
- URL filtering enhancement—The module checks the outgoing URL requests with the policy defined on a Websense Windows NT or UNIX-based server. Depending on the response from the server, which matches a request against a list of 17 website characteristics that are considered inappropriate for business use, the module either permits or denies the connection.
- 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 nonpredictable), port numbers, and additional TCP flags. You can control all inbound and outbound traffic by applying security policies to each connection table entry.

- Performance—With support for up to 6 gigabits of throughput, firewalls can provide protection in the most demanding network environments.

- **Reliability**—Cisco firewalls provide adaptable security services for operation-critical network environments by using the integrated stateful failover capabilities within the Firewall Services Module. Network traffic can be automatically sent 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.
- **Scalability**—Up to two modules are supported in a single Cisco 7600 series router chassis.

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
- PIX Firewall Manager (PFM)
- CSPM
- Conduit
- DHCP client

The front panel LEDs are shown in [Figure 7-1](#) and described in [Table 7-1](#).

Figure 7-1 Firewall Services Module (WS-SVC-FWM-1-K9)

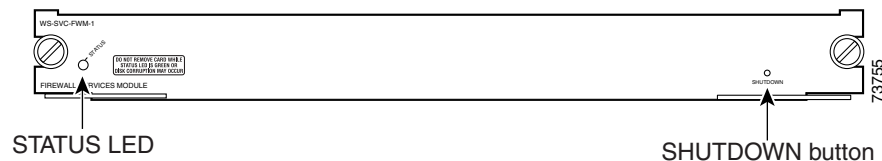


Table 7-1 Firewall Services Module STATUS LED Description

Color/State	Description
Green	All diagnostic tests pass. The module is operational.
Red	A diagnostic test other than an individual port test failed.
Orange	Indicates one of three conditions: <ul style="list-style-type: none"> • The module is running through its boot and self-test diagnostic sequence. • The module is disabled. • The module is in the shutdown state.
Off	The firewall module power is off.

The SHUTDOWN button is used to manually shut down the Firewall Services Module. To prevent corruption of the module, it is critical that the module run through the shutdown procedure before shutting off. If the module fails to respond to CLI or NAM shutdown commands, you can use the SHUTDOWN button as an alternative shutdown method.

For further information on the Firewall Services Module, refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 2.3*.

