Cisco Firewall Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series

Figure 1. Cisco Catalyst 6500 Series and 7600 Series Firewall Services Module

The Cisco® Firewall Services Module (FWSM) for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers is a high-performance, integrated stateful inspection firewall with application and protocol inspection engines. It provides upto 5.5 Gbps of throughput, 100,000 new connections per second, one million concurrent connections or 256,000 NAT translations and upto 80,000 Access Control List Entries. Up to four FWSMs can be installed in a single chassis, providing scalability up to 20 Gbps per chassis. As an extension to the Cisco PIX®/ASA family of security appliances, the FWSM provides large enterprises and service providers with superior security, performance, and reliability.

Based on Cisco PIX/ASA firewall technology, the FWSM is a hardened, embedded system that eliminates security holes and performance-degrading overhead. The Cisco FWSM tracks the state of all network communications and prevents unauthorized network access. It delivers strong application-layer security through intelligent, application-aware inspection engines that examine network flows at Layers 4–7, including market-leading protection for voice over IP (VoIP), multimedia, instant messaging, and peer-to-peer applications.

Flexible Management Options

The Cisco FWSM is managed by the integrated Cisco PIX Device Manager (PDM) for the Cisco FWSM Software v2.3 or earlier, or by the Cisco Adaptive Security Device Manager (ASDM) for Cisco FWSM Software v3.1 or later for device and policy configuration, monitoring, and troubleshooting of a single FWSM. Cisco PDM can be launched from the CiscoWorks CiscoView Device Manager (CVDM) for device provisioning of Cisco Catalyst switches and other services modules. The Cisco FWSM can also be managed from centralized, scalable, multidevice policy-based management tools, including CiscoWorks VPN/Security Management Solution (VMS); the Cisco Security Manager; and the Cisco Security Monitoring, Analysis, and Response System (MARS). Together with other security devices, these central management tools manage the FWSM throughout the network in a consistent manner to best expedite large security deployments.

Security Services Integration

The Cisco FWSM can be combined with other Cisco security services modules such as the Intrusion Detection Services Module (IDSM-2), IP Security (IPSec) VPN Shared Port Adapter (SPA), Traffic Anomaly Detection Module (ADM), Anomaly Guard Module (AGM), and the Network Analysis Module (NAM-1 and NAM-2). Together, these services modules provide a complete self-defending network solution. Integration of service modules into one chassis allows for ease of use and support for network administrators. Role-based remote access controls fosters collaboration for IT managers.

With this modular approach, customers can use their existing switching and routing infrastructures for cost-effective deployment—and can do so while obtaining the highest performance available in the industry and providing secured IP services along with multilayer LAN and WAN switching and routing capabilities.

Firewall Services Module Benefits

Integrated Module Enhances Security and Lowers Cost of Ownership

Besides protecting the perimeter of the corporate network from threats, the Cisco FWSM is installed inside a Cisco Catalyst 6500 Series switch or Cisco 7600 Series router, inspects traffic flows and prevents unauthorized users from accessing a particular subnet, workgroup, or LAN within a corporate network. This intelligent network integration allows the FWSM to provide greater investment protection, a lower total cost of ownership, and a reduced footprint where power and rack space are at a premium. Any physical port on the switch can be configured to operate with firewall policy and protection, allowing for easy deployment without additional configuration and cabling, and providing firewall security inside the network infrastructure. The FWSM can be deployed together with other Cisco Catalyst 6500 Series and Cisco 7600 Series security services modules, for a secure, multilayer defense-in-depth IP services solution.

High Performance, High Scalability and Low Latency Ready for the Future

The FWSM is based on high-speed network processors that provide high performance but retain the flexibility of general-purpose CPUs. The Cisco FWSM provides industry-leading performance of upto 100,000 new connections per second, 5.5 Gbps of throughput, and one million concurrent connections per service module. This superior performance helps organizations meet future growing requirements without requiring a system overhaul. Multiple FWSMs can be clustered using static VLAN configurations or the Catalyst 6500 IOS Policy-based Routing (PBR) for directing traffic to these FWSMs. Up to four FWSMs can be deployed in the same chassis for a total of 20 Gbps throughput. A single FWSM can support up to 1000 virtual interfaces (maximum of 100 per context), and a single chassis can scale up to a maximum of 4000 VLANs. In addition, two Cisco Application Control Engines (ACE) can be used within the Catalyst 6500 chassis to load balance three FWSMs for over 15Gbps of firewall throughput, over 150,000 connections per second and two million concurrent connections.

Full firewall protection is applied across the switch backplane, giving the lowest latency figures (30 microseconds for small frames) possible. This is important to secure latency-sensitive applications such as financial market data and voice over IP (VoIP).

Service Virtualization Reduces Cost and Complexity of Management

The Cisco FWSM provides service virtualization, which allows service providers and large enterprises to implement separate policies for different customers or functional areas, such as multiple demilitarized zones (DMZs), over the same physical infrastructure. Virtualization helps reduce the cost and complexity of managing multiple devices, and makes it easier to add or delete security contexts as subscribers grow. A single FWSM can be partitioned into a maximum of 250 virtual firewalls (security contexts) in Cisco FWSM Software v3.1 or above. FWSM virtualization includes support for Transparent Mode (Layer 2) and Routed Mode (Layer 3). All policies, monitoring and logging are supported in FWSM virtualization which includes Network Address Translation (NAT), access control lists (ACLs), inspection engines, Simple Network Management Protocol (SNMP), syslog, and Dynamic Host Control Protocol (DHCP), and more.

The FWSM Resource Manager helps ensure high availability by limiting resource usage allocated to each security context at any time. This can prevent certain contexts from consuming all resources and denying those resources to other contexts. These resources include number of connections, local hosts, NATs, ACLs, bandwidth, inspection rates, and syslog rates. Role-based management allows multiple IT owners to configure and manage network-and application-layer security policies. Used at the Internet edge, the FWSM can be configured to map virtual firewalls to virtual routing and forwarding instances (VRFs) to provide complete traffic separation and security on the campus network. With the default FWSM software, up to two security contexts and an additional special administrative context are provided. For more security contexts, a license must be purchased.

Ease of Deployment with Transparent (Layer 2) Firewall

The transparent firewall feature configures the FWSM to act as a Layer 2 bridging firewall and requires minimal changes to the network topology. The use of a transparent firewall reduces both the configuration and deployment time. There are no IP addresses except for the management interface; no subnetting or configuration updates are required with transparent firewalls. The transparent firewall feature greatly simplifies deployment in the data center for protecting hosts. The transparent firewalls also fit into existing networks with no Layer 3 changes and transparently pass Layer 3 traffic from routers, allowing interoperability with IP services such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), Multicast, and non-IP traffic such as Internetwork Packet Exchange (IPX), Multiprotocol Label Switching (MPLS), and bridge protocol data units (BPDUs). The transparent firewall is also supported for multiple virtual firewalls. With the release of Cisco FWSM Software v3.1, a mixture of transparent firewall and routed firewall can also be implemented on the same FWSM, providing the most flexible network deployment options. All Layer 3 firewall features are supported with transparent firewall, including NAT and PAT in Cisco FWSM Software v3.2.

High Availability

For network resilience, the Cisco FWSM supports high-speed failover between modules within a single Cisco Catalyst 6500 or Cisco 7600 chassis (intrachassis) and between modules in separate chassis (interchassis), offering customers complete flexibility in their firewall deployments. Cisco FWSM Software v3.1 adds Active-Active stateful failover support in multiple context mode in addition to Active-Standby stateful failover.

Robust Stateful Inspection and Application-Layer Security

The Cisco FWSM is based on the Cisco PIX firewall technology, also known as the Adaptive Security Algorithm (ASA). The FWSM offers rich stateful inspection firewall services, tracking the state of all network communications, applying security policy, and preventing Denial of Service attacks and unauthorized network access. The FWSM creates a connection table entry for a session flow based on the source and destination addresses, randomized TCP sequence numbers, port numbers, and additional TCP flags, and applies security policy to these connections.

Building upon the network-based firewall services, the FWSM also delivers strong application-layer security through intelligent, application-aware inspection engines that examine network flows at Layers 4–7. To defend networks from application-layer attacks, these inspection engines incorporate extensive application and protocol knowledge, and employ security enforcement technologies that include standards conformance checking, protocol anomaly detection, application and protocol state tracking, bidirectional NAT services, bidirectional ACLs, Port Address Translation (PAT), and attack detection and mitigation techniques such as application/protocol command filtering, content verification, URL obfuscation, and URL filtering. These inspection engines give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications. In addition, the FWSM provides market-leading protection for a wide range of VoIP and other multimedia standards.

Cisco FWSM Platform Performance and Capacities

Table 1 provides information on the performance and capacity of the Cisco FWSM.

Table 1. Cisco FWSM Platform Performance and Capacities

	Capacities
Performance	• 5.5 Gbps throughput per service module • Up to 4 FWSMs (20 Gbps) per Catalyst 6500 chassis with static VLAN or IOS Policy-based Routing • 2.8 Mpps • 1 million concurrent connections • 100,000 connection setups and teardowns per second • 256,000 concurrent NAT or PAT translations • Jumbo Ethernet packets (8500 bytes) supported
VLAN Interfaces	• 1000 total per service module • 256 VLANs per security context in routed mode • 8 VLAN pairs per security context in transparent mode
Access Lists	• Up to 80,000 Access Control Entries in single context mode • Note: the FWSM implements Layer 3 and 4 access control security checks in hardware with virtually no performance impact using non-upgradeable high-speed memory
Virtual Firewalls (Security Contexts)	• 20, 50, 100, 250 Virtual Firewall licenses • 2 Virtual Firewalls and 1 administrative context are provided for testing purposes.

FWSM Overall Feature Summary

Table 2 provides an overall feature summary of the Cisco FWSM.

Table 2. FWSM Overall Feature Summary

Features	Summary
Scalable Architecture to Support Up to 20+ Gbps of Firewall Services within the Catalyst 6K Infrastructure	• A variety of industry proven clustering techniques deliver a seamless method to scale firewall performance to 20 Gbps and beyond.
Visibility into Encrypted Threats	• Leveraging SSL decryption capabilities within the Catalyst 6K infrastructure, the FWSM has the ability to gain visibility into encrypted policy violations to which traditional firewalls have no visibility.
Intelligent Network Services	• Layer 2 Firewall (transparent mode) with NAT and PAT support • Layer 2 Firewall (transparent mode) with NAT and PAT support • Layer 3 Firewall (route and/or NAT mode) • Mixed Layer 2 and Lyer 3 firewall per FWSM • Dynamic/static NAT and PAT • Policy-based NAT • VRF-aware NAT • Destination NAT for Multicast • Static routing support in signle- and multiple security content mode • Dynamic routing in single security context mode: Open Shortest Path First (OSPF). Routing Initiation Protocol (RIP) v1 and v2, PIM Sparse Mode v2 multicast routing, Internet Group Management Protocol (IGMP) v2. • Dynamic routing in single and virtual security context mode using stub iBGP (Licensed feature) • Transparent mode supports static routing only • Private VLAN for L2 and L3 firewall enables firewall security policies between isolated ports. • Asymmetric routing supporting without redundancy by using asymmetric routing groups • IPv6 networking and management access using IPv6 HTTPS, Secure Shell Protocol (SSH) v1 and v2, and Telnet
Core Stateful Firewall	• NAT Translate bypass enhances scalability by not creating NAT translate entries when no NAT-control or NAT except is used • Selective TCP State Bypass on a per flow basis • Timeout on a per flow for TCP and non-TCP flows • ACLs: Extended ACL for IP traffic, Ethertype ACL for non-IP traffic, standard ACL for OSPF route distribution, per-user Cisco Secure Access Control Server (ACS)-based ACLs, per-user ACL override, object fgrouping for ACLs, time-based ACLs • Cisco Modular Policy Framework (MPF) with flow-based security policies • Cut-through user authentication proxy with local database and external AAA server support: TCP, HTTP, FTP, HTTPS, and others • URL filtering: Filter HTTP, HTTPS, and FTP requests by Websense Enterprise or HTTP filtering by N2H2 (now part of Secure Computing Corporation) • Same security-level communication between VLANs (without NAT/static policies) and per-host maximum connection limit • Protection from denial of service (DoS) attacks: DNS Guard, Flood Defender, Flood Guard, TCP Intercept with SYN cookies organization, Unicast Reverse Path Forwarding (uRPF), Mail Guard, FragGuard and Virtual Reassembly, Internet Control Message Protocol (ICMP) stateful inspection, User Datagram Protocol (UDP) rate control, TCP stream re-assembly and deobfuscation engine, TCP traffic normalization services for attack detection • Address Resolution Protocol (ARP) inspection in transparent firewall mode • DHCP server, DHCP relay to upstream router with per interface configuration

Features	Summary
Service Virtualization (Multiple Security Context Mode)	• Transparent • Routed Mode • NAT/PAT • ACL • Protocol Inspection • SNMP • Syslog • DHCP • Resource management controls resource usage per security context
Inspection Engines	• Application policy enforcement • Protocol conformance checking • Protocol state tracking • Security checks • NAT/PAT support • Dynamic port allocation • Core internet protocols: HTTP, FTP, Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), DNS, Extended DNS (EDNS), ICMP, TCP, UDP • Database/OS services: Internet Locator Services/Lightweight Directory Access Protocol (ISL/LDAP), Oracle/SQL*Net v1 and v2, NetBIOS over IP, NFS, Remote Shell Protocol (RSH), sUNrpc/nis+, XWindows (SDMCP), Registration Admission and Status (RAS) v2 • Multimedia/VoIP: H.323 v1–4, H.323 Gatekeeper Cluster GUP message support, Session Initiation Protocol (SIP), SCCP (Skinny), Skinny Video, GPRS Tunneling Protocol (GTP) v0 and v1 (3G Mobile Wireless), Media Gateway Control Protocol (MGCP) v0.1 and v1.0, Real-Time Streaming Protocol (RTSP), Telephony Application Programming Interface (TAPI) and Java TAPI (JTAPI) T.38 Fax over IP, Gatekeeper Routed Control Signaling (GKRCS), fragmented and segmented multimedia stream inspection • Specific applications: Microsoft Windows Messenger, Microsoft NetMeeting, Real Player, Cisco IP phones, Cisco SoftPhone • Security services: Point-to-Point Tuneling Protocol (PPTP)
High Availability	• Intrachassis and interchassis • Active-Standby stateful failover • Active-Active stateful failover support in multiple context mode • Asymmetric routing support with Active-Active redundancy
Application Inspection Control	• Advanced HTTP inspection services: RFC compliance checking for protocol anomaly detection, HTTP command filtering, MIME type filtering content validation, Uniform Resource Identifier (URI) length enforcement, and more • Tunneling application control: AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger, peer-to-peer applications (such as KaZaA and Gnutella), and other applications (such as GoToMyPC)
System Management	• Console to command-line interface (CLI): Session from switch, Cisco IOS Software-like CLI parser • Telnet to the inside interface of FWSM • Telnet over IPSec to the outside interface of FWSM • SSH v1 and v2 to CLI • Web GUI-based single device manager (HTTP, HTTPS): Cisco ASDM v5.2F for FWSM 3.2; Cisco ASDM v5.0F for FWSM Software 3.1; Cisco PIX Device Manager 4.1 for FWSM Software 2.3; • Web GUI-based multiple device manager: Cisco Security Manager v3.0 or above for FWSM Software 2.3 or later; CiscoWorks VMS Management Center v1.3 for FWSM Software 2.3 or earlier • Web GUI-based CiscoView Device Manager v1.0 for Cisco Catalyst 6500 to configure FWSM Software 2.3 or earlier and launch Cisco PIX Device Manager • Web GUI-based multiple device manager: CiscoWorks VMS Management Center v1.3 for FWSM Software 2.3 or earlier; Cisco Security Manager for FWSM Software 2.3 • SNMP v2c MIBs and traps • Authenticaiton, authorization, and accounting (AAA): TACACS+ and RADIUS support • Role-based administrative access • Online upgrade • Dedicated out-of-band management interface

Features	Summary
Logging/Monitoring	• Syslog: External servers, up to 16 servers (4 per context) • FTP, URL, ACL logging • SNMP v2c • Multiplatform real-time monitoring, analysis and reporting with Cisco Security Monitoring, Analysis and Response System (MARS) v4.2 for FWSM Software 2.3 or later

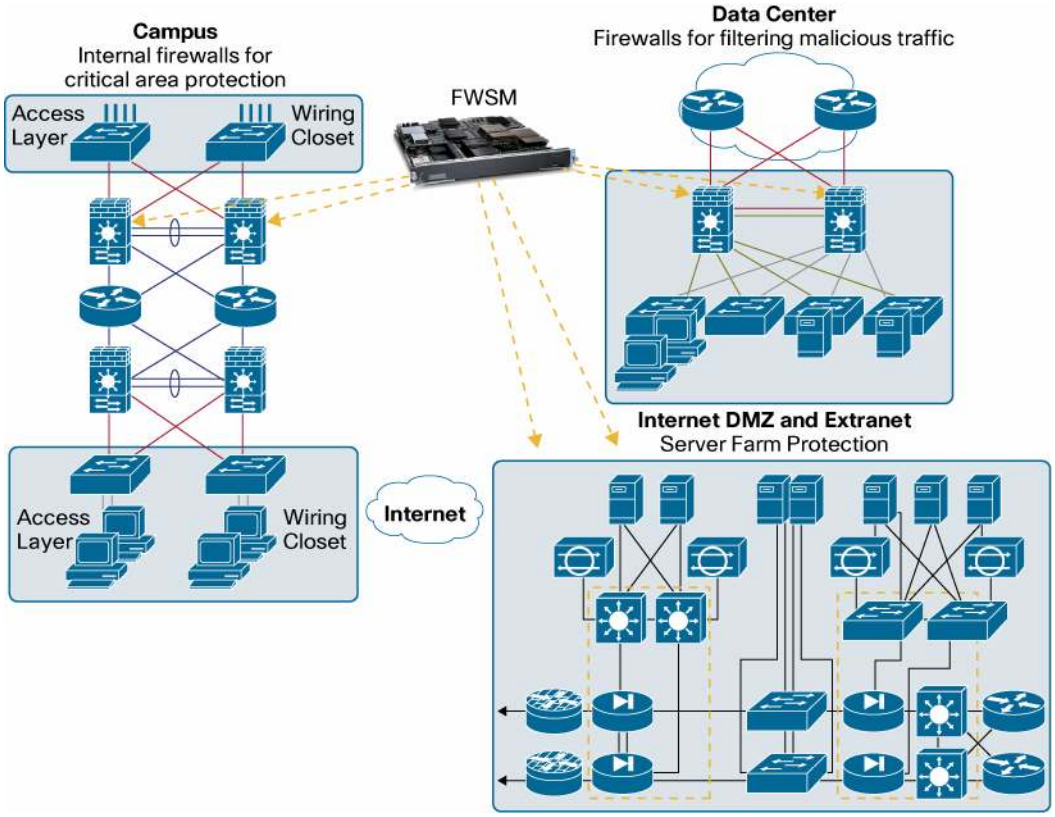
Note: Cisco FWSM Software versions 3.2, 3.1, 2.3, and 2.2 incorporate many of the features from Cisco PIX Security Appliance Software versions 7.0, 6.3, and 6.2, respectively.

Example FWSM Deployments

The Cisco FWSM can be deployed in topologies serving enterprise campuses, data centers, or service providers. The FWSM maximizes capital investment by providing the best price-performance ratio in a firewall.

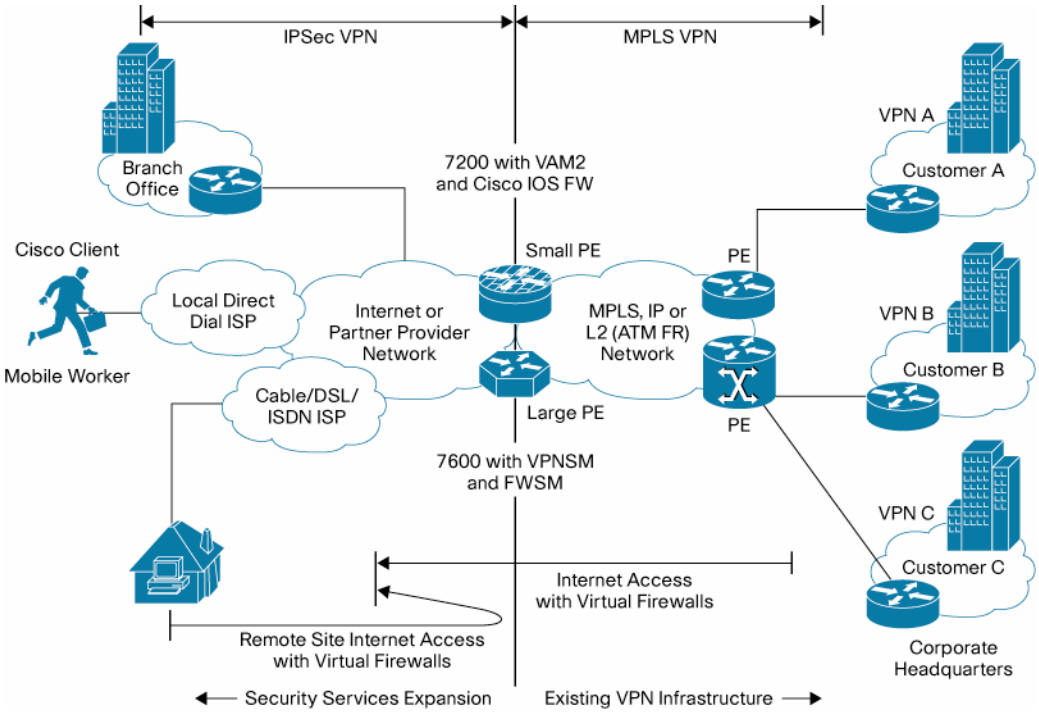
Today's enterprises need more than just perimeter security—they need to connect business partners and provide campus security domains that serve multiple groups within these organizations. The Cisco FWSM provides a flexible, cost-effective, and performance-based solution that allows users and administrators to establish security domains with different policies within the organization. Using the Cisco FWSM, users can set appropriate policies for different VLANs. Data centers also require stateful firewall security solutions to filter malicious traffic and protect data in the Demilitarized zones (DMZ) and extranet server farms. while delivering gigabit performance at the lowest possible cost. Figure 2 shows secured LAN deployments using the Cisco FWSM in the Enterprise campus and data center.

Figure 2. Secure LAN Deployments in the Enterprise Campus and Data Center



At the Enterprise or Service Provider WAN edge, the FWSM can also be combined with the Cisco IPSEC VPN SPA to enforce firewall policies per VPN tunnel defined by VRF.

Figure 3. Secure WAN Deployments in the WAN Edge



Ordering Information

Table 3. Cisco Firewall Services Module Hardware and Software Part Numbers

Product Number	Description
Hardware	
WS-SVC-FWM-1-K9	Firewall Services Module for Cisco Catalyst 6500 and 7600 Series
WS-SVC-FWM-1-K9=	Firewall Services Module for Cisco Catalyst 6500 and 7600 Series (spare)
Security Bundles	
WS-C6506-E-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis and Supervisor 720 3B
WS-C6509-E-FWM-K9	Cisco Catalyst 6509 Firewall Security System with Enhanced Chassis and Supervisor 720 3B
WS-C6513-FWM-K9	Cisco Catalyst 6513 Firewall Security System with Supervisor 720 3B
WS-6509EXL-2FWM-K9	Cisco Catalyst 6509 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and two Firewall Service Modules
WS-6513XL-2FWM-K9	Cisco Catalyst 6513 Firewall Security System with Supervisor 720 3BXL and two Firewall Service Modules
WS-6506-EXL-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
WS-6509-EXL-FWM-K9	Cisco Catalyst 6506 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
WS-C6513-XL-FWM-K9	Cisco Catalyst 6513 Firewall Security System with Enhanced Chassis, Supervisor 720 3BXL and one Firewall Service Module
Software	
SC-SVC-FWM-1.1-K9	Firewall Services Module Software Release 1.1 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-1.1-K9=	Firewall Services Module Software Release 1.1 for Cisco Catalyst 6500 and 7600 Series (spare)
SC-SVC-FWM-2.2-K9	Firewall Services Module Software Release 2.2 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-2.2-K9=	Firewall Services Module Software Release 2.2 for Cisco Catalyst 6500 and 7600 Series (spare)
SC-SVC-FWM-2.3-K9	Firewall Services Module Software Release 2.3 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-2.3-K9=	Firewall Services Module Software Release 2.3 for Cisco Catalyst 6500 and 7600 Series (spare)
SC-SVC-FWM-3.1-K9	Firewall Services Module Software Release 3.1 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-3.1-K9=	Firewall Services Module Software Release 3.1 for Cisco Catalyst 6500 and 7600 Series (spare)
SC-SVC-FWM-3.2-K9	Firewall Services Module Software Release 3.2 for Cisco Catalyst 6500 and 7600 Series
SC-SVC-FWM-3.2-K9=	Firewall Services Module Software Release 3.2 for Cisco Catalyst 6500 and 7600 Series (spare)

Note: Cisco Firewall Services Module Software 1.1 has reached end-of-sale status. Customers are encouraged to upgrade or purchase FWSM Software 2.3 or 3.1, 3.2.

Licensing

Table 4 lists the part numbers that are needed when ordering virtual firewall (security context) licenses. To be able to order any of these license tiers, you must be running FWSM Software 2.2(1) or higher. No changes in hardware are required when upgrading from FWSM Software 1.1 to versions 2.2, 2.3 and 3.1, 3.2

Table 4. Context License Part Numbers

Part Number	Description
FR-SVC-FWM-VC-T1	20 virtual firewall licenses for Cisco FWSM Software 2.2 or above
FR-SVC-FWM-VC-T2	50 virtual firewall licenses for Cisco FWSM Software 2.2 or above
FR-SVC-FWM-VC-T3	100 virtual firewall licenses for Cisco FWSM Software 2.2 or above
FR-SVC-FWM-VC-T4	250 virtual firewall licenses for Cisco FWSM Software 3.1 or above
FR-SVC-FWM-UPGR1	Upgrade from 20 to 50 virtual firewalls for Cisco FWSM Software 2.2 or above
FR-SVC-FWM-UPGR2	Upgrade from 50 to 100 virtual firewalls for Cisco FWSM Software 2.2 or above
FR-SVC-FWM-UPGR3	Upgrade from 100 to 250 virtual firewalls for Cisco FWSM Software 3.1, 3.2

Table 5. GTP/GPRS Mobile Wireless Inspection Licenses

Part Number	Description
FR-SVC-FWM-GTP	GTP Protocol Inspection Engine license for Cisco FWSM Software 3.1, 3.2

Table 6. System Requirements

Support for FWSM 3.1, 3.2	
	Supervisor Engines[1]
Cisco IOS	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	2, 720, 32
Catalyst OS[2]	
8.5(3) and higher	2, 720, 32

Support for FWSM 2.3 and 2.3			
		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 and higher	2, 720	No	No
12.2(17a)SX3	2, 720	**Yes**	**Yes**

[1] The FWSM does not support the supervisor 1 or 1A. FWSM supports Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2), Supervisor 32 or Supervisor 720.
[2] Supports multiple switched VLAN interfaces (SVIs) between the Multilayer Switch Feature Card (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. Other releases that do not support BPDU forwarding only support transparent mode without failover.

Support for FWSM 2.3 and 2.3			
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) and higher	2, 720	**Yes**	**Yes**
8.3(x)	2, 720	**Yes**	**Yes**

Table 7. Product Specifications

Product	Specifications
Hardware Specification	• Weight: 10 lb • Power Consumption: 171.78W
Regulatory Compliance	**Safety** • UL 1950 • CSA C22.2 No. 950-95 • EN60950 • EN60825-1 • TS001 • CE Marking • IEC 60950 • AS/NZS3260 **Telecommunications** • ITU-T G.610 • ITU-T G.703 • ITU-T G.707 • ITU-T G.783 Sections 9-10 • ITU-T G.784 • ITU-T G.803 • ITU-T G.813 • ITU-T G.825 • ITU-T G.826 • ITU-T G.841 • ITU-T G.957 Table 3 • ITU-T G.958 • ITU-T I.361 • ITU-T I.363 • ITU I.432 • ITU-T Q.2110 • ITU-T Q.2130 • ITU-T Q.2140 • ITU-T Q.2931 • ITU-T O.151 • ITU-T O.171 • ETSI ETS 300 417-1-1 • TAS SC BISDN (1998) • ACA TS 026 (1997) • BABT/TC/139 (Draft 1e) **EMI** • FCC Part 15 Class A

[4] When you use Catalyst OS on the supervisor, you can use any of the supported Cisco IOS releases above on the MSFC. The supervisor software determines the FWSM feature support.
Autostate feature for rapid link failure detection is supported with Cisco Catalyst OS Release 8.4(1) or later and Cisco IOS 12.2(18)SXF(5) and higher.

Product	Specifications
	• ICES-003 Class A • VCCI Class B • EN55022 Class B • CISPR22 Class B • CE Marking • AS/NZS3548 Class B **Common Criteria** • EAL4+ **NEBS** • SR-3580—NEBS: Criteria Levels (Level 3 compliant) • GR-63-CORE—NEBS: Physical Protection • GR-1089-CORE—NEBS: EMC and Safety **ETSI** • ETS-300386-2 Switching Equipment

For More Information

For more information, contact your local account representative or visit:

- Detailed Cisco FWSM Specifications: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/fwsm_3_1/fwsm_cfg/specs_f.htm#wp1002608
- Cisco security solutions: http://www.cisco.com/en/US/partner/products/hw/vpndevc/index.html
- Cisco PIX Security Appliance Software: http://www.cisco.com/go/pix
- Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm
- Cisco Catalyst 6500 Series: http://www.cisco.com/en/US/products/hw/switches/ps708/index.html
- Cisco 7600 Series: http://www.cisco.com/en/US/products/hw/routers/ps368/index.html
- CiscoWorks VMS Management Center for Firewalls: http://www.cisco.com/en/US/products/sw/cscowork/ps2330/
- Cisco Security MARS: http://www.cisco.com/en/US/products/ps6241/index.html
- Cisco Security Manager: http://www.cisco.com/en/US/products/ps6498/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-383290-03 10/10