PRODUCT BULLETIN NO. 2518

# CISCO FIREWALL SERVICES MODULE SOFTWARE RELEASE 2.2(1) FOR CISCO CATALYST 6500 SWITCHES AND CISCO 7600 SERIES ROUTERS

**The Firewall Services Module (FWSM) is an integrated security module for Cisco® Catalyst® 6500 Series switches and 7600 Series routers that provides stateful Layer 7 filtering capabilities. Cisco is announcing FWSM Software Release 2.2(1). The major new features supported in this release include virtualization at Layers 2 and 3 and resource management.**

The Self-Defending Network is Cisco Systems' long-term strategy to allow organizations to identify, prevent, and adapt to threats using security that is integrated into all aspects of their connected business processes—incorporating secure connectivity, threat defense, and trust and identity technologies. The FWSM is a critical element of the Cisco Threat Defense System—its unique integration of robust security services with network intelligence offers scalable, resilient protection from threats.

Investment protection is the primary metric by which all next-generation switches are judged. No longer are CEOs and CIOs seeking to perform wholesale equipment replacements for performance upgrades within their networks. Equipment vendors will be required to perform upgrades to equipment by simply changing switch fabrics and adding additional higher-performance line modules. The FWSM helps to preserve a company's existing investment in Cisco Catalyst switches by adding to the existing devices, rather than rebuilding the entire network for security purposes

Network virtualization blends the economics and efficiencies of shared systems with the integrity, performance, and security of independent systems. The virtualized FWSM delivers multiple firewalls on one physical hardware platform. Network administrators can configure, deploy, and manage these firewalls as if they were separate devices. They can also partition and manage resources independently, and allocate different quantities to specific applications.

Network virtualization technology allows corporations to not only increase network resource usage and exert more control over resources and their allocation, but also to gain flexibility and speed in scaling the resources. Using virtualization to reduce the number of physical devices in a network significantly reduces the cost and complexity of managing a network infrastructure.

Cisco FWSM Software 2.2(1) includes the features listed in Table 1.

**Table 1.** Cisco FWSM Software 2.2(1) Features

| Feature | Description |
|---|---|
| **Virtualization (Security Contexts)** | Allows the customer to split a single Cisco FWSM into multiple logical security contexts. Two security contexts come free as part of the base software release. For additional security contexts, you need to buy the appropriate licenses.<br>At Layer 3, the virtualization feature supports:<br>• 100 security contexts<br>• 1000 interfaces (maximum per FWSM)<br>• 256 interfaces per virtual security context<br>• 250 interfaces for failover tracking interfaces |
| **Transparent Firewall** | Known as a Layer 2 firewall or "stealth firewall." It is not seen as a router hop to connected devices. In Layer 2, this feature supports:<br>• 100 transparent security contexts<br>• Two interfaces per transparent firewall<br>• Layer 2 access control lists (ACLs) |

| Feature | Description |
|---|---|
| | • Address Resolution Protocol (ARP) inspection<br>• Multicast passthrough<br>• No Network Address Translation (NAT)<br>• No outside shared VLAN<br>• One management IP address per transparent firewall context<br>• The same subnet, but different VLAN tags on the inside and outside |
| **Resource Manager** | By default, all security contexts have unlimited access to the resources of the FWSM, except where maximum limits per context are enforced. The limits for individual resources can be defined as a percentage or as an absolute value. Following are the resources that may be limited:<br>• mac-address<br>• cons<br>• fixups<br>• hosts<br>• ipsec<br>• ssh<br>• syslogs<br>• telnet<br>• xlates |
| **Bidirectional and Policy-based NAT** | Address translation is applied to addresses of hosts residing on the outer (less secure) interfaces of the FWSM. This:<br>• Enables connectivity between networks with overlapping IP addresses<br>• Allows outside dynamic NAT to be enabled on an interface; an explicit NAT policy must be configured for all hosts on the interface<br>• Policy-based NAT lets you identify local traffic for address translation by specifying the source and destination addresses (or ports) in an access list. Regular NAT uses source addresses and ports only, whereas Policy-based NAT uses both source and destination addresses and ports. |
| **VoIP Protocols** | H.323 versions 3 and 4 use the following User Datagram Protocol (UDP) ports:<br>• 1718<br>• 1719<br>• 1720<br>This adds support for many new H.323 features, including the ability to handle multiple calls<br>that use the same call signaling channel. Also supported:<br>• Media Gateway Control Protocol (MGCP) Version 1.0 (no NAT or Port Address Translation [PAT])<br>• PAT for Session Initiation Protocol (SIP)<br>• Skinny Inspection Engine<br>• Real-Time Streaming Protocol (RTSP) |

| Feature | Description |
|---|---|
| **Syslog** | The FWSM supports traps and Simple Network Management Protocol (SNMP) get requests,<br>but does not support SNMP set requests.<br>The following MIBs are supported<br>• SNMP core traps<br>• MIB-II<br>• Firewall MIB<br>• Memory Pool MIB<br>• Process MIB<br>• Syslog MIB |
| **Multiple Switched Virtual Interfaces** | Cisco FWSM Software 2.2(1) allows multiple VLANs between the Multilayer Switch Feature Card (MSFC) and the FWSM. This is valuable in specific deployment scenarios (in transparent firewalls, for example). |
| **Allow Communication Between Interfaces of Same Security Levels** | By default, interfaces on the same security level cannot communicate with each other, but with FWSM Software 2.2(1), this behavior is configurable. This feature can be used where you want protection features to be applied equally for traffic between two interfaces; for example, if you have two departments that are equally secure, or you would like to assign more than 100 interfaces in a security context. |
| **Dynamic Host Control Protocol (DHCP) Relay** | Forwards DHCP requests from devices on specific interfaces to an administrator-specified DHCP server. Providesa method for enterprises to centrally distribute, track, and maintain IP addresses. |
| **Assignable Syslog Levels by Message** | Allows you to decide which syslog messages eventually get generated. |
| **Internet Control Message Protocol (ICMP) Stateful Inspection** | Allows stateful inspection of ICMP. The ICMP payload is scanned to retrieve the five-tuple from the original packet. The ICMP inspection engine supports one-to-one NAT and PAT. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. |
| **Online Upgrade** | FWSM software can be upgraded to a different minor maintenance version while failover is still active. You can use different maintenance versions (third number) during an upgrade process;<br>for example, you can upgrade one unit from 2.2(1) to 2.2(2) |
| **N2H2 Support** | In addition to WebSense, N2H2 has also been added for URL filtering purposes. The maximum number of URL servers is limited to four per contexts. |
| **Network Management Support** | The following network management solutions are supported:<br>• Command-line interface (CLI)<br>• Cisco PIX® Device Manager Version 4.0<br>• MC 1.3.1 |

## LICENSING

Cisco FWSM Software 2.2(1) includes two free security contexts as part of the software release. If you purchased Cisco SMARTnet(r) support, you should be able to download Cisco FWSM Software 2.2(1) from Cisco.com and to use two security contexts in addition to the special admin context. More security contexts (inclusive of two contexts) are available in tiers of 20, 50, and 100 virtual firewalls. Table 2 lists the part numbers for the licenses.

**Table 2.** Part Numbers for Cisco FWSM Software 2.2(1) Security Contexts

| Part Number | Product Description |
|---|---|
| FR-SVC-FWM-VC-T1 | 20 virtual firewalls |
| FR-SVC-FWM-VC-T2 | 50 virtual firewalls |
| FR-SVC-FWM-VC-T3 | 100 virtual firewalls |

Table 3 lists upgrade part numbers for Cisco FWSM Software 2.2(1) security contexts.

**Table 3.**

| Part Number | Product Description |
|---|---|
| FR-SVC-FWM-UPGR1 | Upgrade from 20 to 50 virtual firewalls |
| FR-SVC-FWM-UPGR2 | Upgrade from 50 to 100 virtual firewalls |

## PLATFORM REQUIREMENTS

Cisco FWSM Software 2.2(1) is supported on Cisco Catalyst 6500 Series switches and 7600 Series routers. For detailed information about minimum supervisor engine operating system requirements, review the Cisco FWSM Software 2.2(1) documentation and release notes.

## AVAILABILITY

Cisco FWSM Software 2.2(1) can be downloaded from the Cisco.com Software Center at:

http://www.cisco.com/kobayashi/sw-center/index.shtml

## PRODUCT INFORMATION

For additional product information, go to:

www.cisco.com/go/tds

## ADDITIONAL INFORMATION

For additional product ordering and availability information, send an e-mail message to:

ask-c6000-pm@cisco.com or cs-fwsm@cisco.com


**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe



204064_ETMG_WH_05.04