What’s New in Cisco Firewall Services Module Software Version 3.2 and Cisco Adaptive Security Device Manager Version 5.2F

PB385035

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 5.5 Gbps of throughput; 100,000 connections per second; and one million concurrent connections. Additionally, clustering solutions with the FWSM can seamlessly deliver more than 20 Gbps of throughput per chassis. Cisco FWSM Software Version 3.2 is configured and monitored by the integrated, Web-GUI-based Cisco Adaptive Security Device Manager (ASDM) Version 5.2F. For remote multidevice management, Cisco FWSM Software Version 3.2 is configured and managed by Cisco Security Manager Version 3.1.

Cisco FWSM Software Version 3.2 provides:

- Core firewall enhancements
- Additional intelligent network services
- Management enhancements
- Cut-through proxy enhancements
- Voice and mobile inspection engine enhancements

Cisco FWSM Software Version 3.2 Release Highlights

Table 1 lists new features in Cisco FWSM Software Version 3.2.

Table 1. New Features in Cisco FWSM Software Version 3.2

Features	Benefits
Core Firewall Enhancements	
Network Address Translation (NAT) bypass	Enhances scalability by not creating NAT translate entries when no NAT control or NAT exempt is used.
Selective TCP state bypass	Selectively bypass TCP state checks for configured traffic classes. This is useful for allowing certain traffic to flow through in asymmetric routing scenarios when two FWSMs are in different locations that are not Layer 2-adjacent.
BGP Stub	New License feature Allows interoperability with a single BGP Peer that enables dynamic routing in single and virtual firewall modes. Not available in transparent firewall
Timeout on a per-flow basis for non-TCP flows	Cisco FWSM Software Version 3.1 provides timeout on a per-flow basis for TCP flows. Version 3.2 adds non-TCP flow support for timeout per flow.
Intelligent Network Services	
Transparent Network and Port Address Translation (NAT and PAT)	Provides NAT and PAT support in transparent firewall mode. This simplifies network configuration for upstream routers, especially in a multiple-ISPs scenario.

Features	Benefits
Dynamic Host Control Protocol (DHCP) relay per interface	Allows DHCP relay to be configured on a per-interface basis.
Management Enhancements	
Additional Simple Network Management Protocol (SNMP) MIBs in single and multiple context modes	Additional MIBs include connection entries, translate entries, Internet Group Management Protocol (IGMP) entries, Resource Manager MIBs for current usage, peak usage and configured thresholds for a given resource, firewall synchronization success/failure, context keepalive, service module keepalive, and performance statistics.
Additional SNMP traps in single and multiple context modes	Additional traps include Resource Manager traps when configured resource thresholds are exceeded, NAT/PAT entries are exhausted, access control list (ACL) memory space is exhausted, CPU threshold is exceeded, and failover has occurred.
TACACS+ command authorization enhancements	Eases management by making TACACS+ string parsing logic to be more like Cisco IOS® Software.
Authentication, authorization, and accounting (AAA) in system context	Enables an administrator who sessions into FWSM system contexts from the Cisco Catalyst 6500 Series supervisor engine to inherit command authentication and authorization from the administrative context.
Cut-Through Proxy Enhancements	
DNS hostname instead of IP address for HTTP POST commands	Provides additional flexibility for cut-through proxy policies.
Connection tear-down as a configurable option when absolute user authentication timer expires	Provides greater levels of detail for state handling.
Expired password handling with TACACS+ and RADIUS server	Provides the ability to distinguish and redirect users with expired passwords to different Webpages.
Customizable redirect Webpage	Provides option for the redirect Webpage to be a local file stored in the Cisco FWSM.
Re-authentication behavior option	Provides support to keep a user authenticated and to not re-prompt for username and password if the user has already been authenticated.
Virtual Secure Shell (SSH) support	Provides a non-GUI method to authenticate with encrypted credentials.
Voice and Mobile Inspection Engine Enhancements	
Real-Time Streaming Protocol (RTSP) PAT	Provides PAT support for the RTSP protocol, including interoperability with all major media players.
Session Initiation Protocol (SIP) enhancements	Enables proper RTP teardown and timeout for better billing and provisioning
H.323 gatekeeper cluster Gatekeeper Update Protocol (GUP) messages support	Ensures interoperability between Cisco Unified CallManager 4.1 and the Cisco FWSM.
GPRS Tunneling Protocol (GTP) enhancement for global GPRS Support Node (GSN) load balancing	Allows the GTP inspection engine to respond to valid GSNs configured for load balancing to enable scalability for mobile 3G networks.

Cisco ASDM Version 5.2F Release Highlights

Cisco ASDM Version 5.2F supports all the new configuration features of Cisco FWSM Software Version 3.2, as well as the new GUI, policy table, and syslog enhancements from Cisco ASDM Version 5.2. Table 2 lists the new features in Cisco ASDM Version 5.2F.

Table 2. New Features in Cisco ASDM 5.2F

Features	Benefits
New Rule Table	
Streamlined policy creation	Provides easy access to all items needed for ACL management, including easy object group and policy creation and modification, policy visualizer, option to expand and display elements in an object group, and ability to see attributes of object and object group.
Policy query	Gives administrators advanced search capabilities for their ACLs.
Syslog Enhancements	
Rule table and syslog integration	Enables single-click rule creation from syslog and instant viewing of syslogs being generated based on a selected ACL. Provides explanation of syslog messages and recommended actions.
New syslog viewer	Enables syslog parsing for customizing views based on time, date, syslog IDs, and IP addresses; and coloring of logs based on severity.
Better Configuration Support	
New object group selector panel eases configuration	Enables rapid editing of network, service, protocol, and ICMP-type object groups.

New Security Bundles for FWSM

Two new security bundles are available for the Cisco FWSM (Table 3). These security bundles include two FWSMs for 10-Gbps firewall throughput or high-availability design. Multiple FWSMs can be clustered using either static VLAN configurations or Cisco IOS Software policy-based routing for directing traffic to these FWSMs. Additional FWSMs can be configured with these security bundles for up to four FWSMs in the same chassis, delivering a total of greater than 20 Gbps firewall throughput.

These security bundles include the Cisco Catalyst 6500 Series Supervisor Engine 720 3BXL, which provides higher performance routing and NetFlow entries than the Supervisor Engine 720 3B. The Supervisor Engine 720 3BXL is ideal for high-performance data center designs. More information about the Supervisor Engine 720 family is available at http://www.cisco.com/en/US/products/hw/modules/ps4835/products_data_sheet09186a0080159856.html.

Table 3. New Security Bundles for FWSM

Part Number	Description
WS-6509EXL-2FWM-K9	Cisco Catalyst 6509 Firewall Security System with Enhanced Chassis, Supervisor Engine 720 3BXL, and two Firewall Services Modules.
WS-6513XL-2FWM-K9	Cisco Catalyst 6513 Firewall Security System with Supervisor Engine 720 3BXL and two Firewall Services Modules.

For More Information

For more information, please visit the following links:

- **Cisco FWSM**: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
- **Cisco ASDM**: http://www.cisco.com/go/asdm
- **Cisco Security Manager**: http://www.cisco.com/en/US/products/ps6498/index.html

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C25-385035-01 08/07