Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 3.1

July 2006

These release notes describe the features and caveats for the Firewall Services Module (FWSM) software release 3.1. This document includes the following sections:

- Important Notes, page 2
- Upgrading the Software, page 2
- Chassis System Requirements, page 2
- Management Support, page 3
- New Features, page 3
- Software License Information, page 9
- Limitations and Restrictions, page 9
- Open Caveats in Software Release 3.1(3), page 10
- Resolved Caveats in Software Release 3.1(2), page 16
- Resolved Caveats in Software Release 3.1(2), page 16
- Related Documentation, page 17
- Obtaining Documentation, page 18
- Documentation Feedback, page 19
- Cisco Product Security Overview, page 19
- Obtaining Technical Assistance, page 20
- Obtaining Additional Publications and Information, page 22

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Important Notes

- You must install maintenance software Release 2.1(2) before you upgrade to FWSM Release 3.1. See the *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1* for detailed information about upgrading to 2.1(2).
- For traffic that passes through the control-plane path, such as packets that require Layer 7 inspection or management traffic, the FWSM sets the maximum number of out-of-order packets that can be queued for a TCP connection to 2 packets, which is not user-configurable. Other TCP normalization features that are supported on the PIX and ASA platforms are not enabled for FWSM.

Upgrading the Software

See the *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1* for detailed information about upgrading to Release 3.1.

Chassis System Requirements

The switch models that support the FWSM include the following platforms:

- Catalyst 6500 series switches, with the following required components:
  - Supervisor engine with Cisco IOS software (known as supervisor IOS) *or* Catalyst operating system (OS). See Table 1 for supported supervisor engine and software releases.
  - MSFC 2 with Cisco IOS software. See Table 1 for supported Cisco IOS releases.
- Cisco 7600 series routers, with the following required components:
  - Supervisor engine with Cisco IOS software. See Table 1 for supported supervisor engine and software releases.
  - MSFC 2 with Cisco IOS software. See Table 1 for supported Cisco IOS releases.

Note The FWSM does not support a direct connection to a switch WAN port because WAN ports do not use static VLANs. However, the WAN port can connect to the MSFC, which can connect to the FWSM.

Table 1 shows the supervisor engine version and software. Please also consult and check the switch software requirements.

Table 1 Support for FWSM 3.1

	Supervisor Engines[1]
Cisco IOS	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	2, 720, 32
Cisco IOS Software Modularity	
12.2(18)SXF4	720, 32
Catalyst OS[2]	
8.5(3) and higher	2. 720, 32

[1] The FWSM does not support the supervisor 1 or 1A.

2. When you use Catalyst OS on the supervisor, you can use any of the supported Cisco IOS releases above on the MSFC. (When you use Cisco IOS software on the supervisor, you use the same release on the MSFC.)

Management Support

The FWSM supports the following management methods:

- Cisco ASDM—Software Release 5.0F supports FWSM software release 3.1 features. ASDM is a browser-based configuration tool that resides on the FWSM. The system administrator can configure multiple security contexts. If desired, individual context administrators can configure only their contexts.
- Command-line interface (CLI)—Access the CLI by sessioning from the switch or by connecting to the FWSM over the network using Telnet or SSH. The FWSM does not have its own external console port.

New Features

Table 2 lists the new features for FWSM software release 3.1.

Table 2 FWSM 3.1 Enhancements

Type of Feature	Feature	Description/Benefits
Authentication, Authorization, and Accounting (AAA)	Support for simultaneous RADIUS accounting servers	Ability to send START/STOP accounting records to multiple RADIUS servers simultaneously. Provides higher scalability for RADIUS accounting.
	Accounting for management traffic	AAA accounting records are generated for management connections to the box. Only TACACS+ is supported. Allows backtracking of administrative commands that may have caused problems.
	Configure FTP authentication challenge	Specifies if the user should be challenged for FTP traffic based on prior authentication of other interactive traffic (telnet, http, https) and whether to challenge and block unauthorized FTP traffic. This allows traffic from internal authenticated hosts to go through, while blocking traffic from unauthenticated users.
	MAC-based AAA exemption	Allows specifying AAA exemption based on a MAC and an IP address that was dynamically allocated or relayed by the DHCP server or DHCP Relay. This supports dynamic addressing of devices like printers and IP phones behind a firewall.
	Cut-through proxy authentication using local database	Authentication of cut-through traffic using a local username database, as a backup for AAA services. This allows disconnected use of policies when an AAA server is not available.

Table 2 FWSM 3.1 Enhancements (continued)

Type of Feature	Feature	Description/Benefits
Access Lists	Time-based ACE	Defines a time range (time of the day and week) when certain ACEs become active. Provides more granular policy, identical to the Cisco IOS software implementation.
	Modular Policy Framework	Provides a modular and consistent framework that identifies traffic flows, classifies traffic, and defines policies. Policies include inspection policies, connection policies, and TCP connection timeouts. The Modular Policy Framework lets you apply these policies to specific classes of traffic.
	Access list editing	ACEs can be added in the middle of a access list between two consecutive ACEs based on the ACE line number. This allows more flexible policy definitions.
	Interface keyword as address in access lists	Allows the use of the **interface** keyword with the **access-list** command.
Network Address Translation	NAT control	NAT configuration is no longer required to pass traffic through the FWSM.
	Overlapping static NAT configuration	Overlapping static statements are allowed and only a warning message is issued. FWSM performs the Longest Prefix lookup for the static statements.
Inspection Engines (Fixups)	TCP stream assembly for application inspection	Assembly of VoIP/TCP streams which are processed by the inspection engines (such as SIP, Skinny, and MGCP) instead of individual packets. This allows interoperability with the latest version of Cisco CallManager.
	Persistent TCP connections and TCP pools for URL filtering	The FWSM uses established connections for requests instead of creating a new TCP connection to the URL server for each HTTP request. It creates a pool of five connections and reuses them in round robin fashion. This improves the performance of Websense and N2H2 URL filtering.
	Configurable application inspection engines	Inspection engines can be enabled for specific interfaces or globally (the **fixup** command has been renamed **inspect**). This provides more granular control of application inspection.
	ESMTP application inspection	Extended SMTP (ESMTP) allows e-mail that includes graphics, audio, video, and text in various national languages. SMTP is still supported in accelerated mode. This enhances client-to-server communication.
	FTP command filtering	Strict FTP inspection includes FTP command request filtering for over ten FTP commands. This provides additional security, including hiding the reply to the **system** command and protecting against username discovery. This feature also provide more granular control of FTP.
	Active X/Java filtering	Filters objects, such as ActiveX objects or Java applets, that may pose security risks.
	PPTP PAT and application inspection enhancement	PAT support and stateful inspection is added for PPTP so that only TCP port 1723 needs to be opened. This simplifies FWSM configuration for remote client connections.

Table 2 FWSM 3.1 Enhancements (continued)

Type of Feature	Feature	Description/Benefits
VoIP Inspection Engines (Fixups)	H.323 enhancement - T.38	Allows inspection and modification of T.38 (FAX over IP) within H.323 sessions. This protects FAX messages transmitted between endpoints over an IP network.
	H.323 enhancement -GKRCS	GKRCS application inspection opens pin-holes between endpoints, which allows firewalls to be placed between an H.323 gatekeeper and the end points.
	MGCP NAT	Supports NAT of the IP address and opening pin-holes according to the NATed/PATed IP address and port information. This allows firewalls to be placed between media gateways and end points.
	GTP application inspection	GTP application inspection provides advanced stateful inspection capabilities for GSM/GPRS wireless service provider (3GPP) environments.
	SIP instant messaging application inspection	Provides Instant Messaging (IM) support for RTC client for Windows Messenger version 4.7.0105. Support for new SIP methods MESSAGE/INFO and new response 202 as described by RFC 3428 and RFC 3265. Allows stateful inspection of IM over SIP.
	TAPI/CTIQBE application inspection	TAPI/CTIQBE application inspection translates the embedded IP addresses or port numbers and opens pinholes for subsequent media transmission between call endpoints. CTIQBE is a VoIP protocol developed by Cisco for Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications for call setup with Cisco CallManager.
	Skinny video support	Supports Skinny (SCCP) video application inspection by handling Skinny video messages that carry embedded IP addresses and ports for the video channels and by opening pinholes for video RTP/RTCP streams. Interoperates with video over IP in Cisco Call Manager 4.0.

Table 2 FWSM 3.1 Enhancements (continued)

Type of Feature	Feature	Description/Benefits
Application Firewall	HTTP inspection engine enhancements	Provides deep payload inspection of HTTP traffic to detect and block Port 80 misuse and deter web-based attacks.
	Detect and block applications and attacks tunneled over HTTP	Detects a list of pre-defined port 80 tunneling applications, such as instant messaging (AIM, MSN Messenger, Yahoo), and peer-to-peer (Kazaa). Permits or blocks traffic based on user policy configured using the Modular Policy Framework. Also generates a message for any port 80 misuse event. Prevents malicious applications from being tunneled over HTTP.
	RFC compliance checking	Specifies whether all traffic that is not compliant with the HTTP standard should be permitted or logged. This provides HTTP protocol anomaly detection.
	HTTP command filtering	Determines if the Request Message is an RFC-defined method (OPTIONS, GET, HEAD, POST, PUT,DELETE, TRACE, or CONNECT) or an extension method (INDEX, MOVE, and so forth.). If the check fails, the user may be alerted, a message may be generated, and the TCP connection may be reset. This lets you select the HTTP methods to allow or deny.
	MIME type filtering	Permits passing a predefined list of mime-types (such as image/Jpeg, text/html, application/msword, audio/mpeg) or all mime-types through the firewall. This helps control the types of content that can traverse the firewall.
	Checks for minimum and maximum size of HTTP message, header length and URI	Permits or denies traffic based on whether a requestor response HTTP message meets the configured size constraints. Checks the maximum header length for the HTTP request and response messages and checks the maximum size of URI permitted through the firewall. Allows control of HTTP messages that violate the criteria defined for URI length and request/response message header size.
	Content validation	Verifies that the content-type specified in the header matches the content-type defined in the body of the HTTP message. Validates that the content-type in the response message matches the request message accept-type field. If the check fails, the user may be alerted, a message may be generated, and the TCP connection may be reset.
	HTTP message filtering based on keywords	Filters HTTP messages based on keywords and takes appropriate action. Improves control and deters port 80 misuse.
High Availability	Active/active	Contexts can be active on one blade, standby on the second blade, while other contexts are in standby in the first blade and active in the second blade. This provides high resilience in multi-group HSRP style.
	Pre-empt option for active/active	Allows redundant FWSMs to preempt one another depending on the configured priority. Allows the design of deterministic traffic paths with redundant firewalls.
	Asymmetric routing support	Traffic that arrives on a different unit or interface than the traffic originated can be forwarded to the unit or interface where the traffic originally was passed. This provides resilient WAN connectivity.

Table 2 FWSM 3.1 Enhancements (continued)

Type of Feature	Feature	Description/Benefits
Scalability	Support for 250 virtual contexts	Maximum number of supported virtual contexts is increased from 100 to 250. This provides high scalability for virtual contexts.
	Apply the **write mem** command to all contexts	The **write mem** command saves configuration for all contexts without having to enter the command for each individual context. This makes configuring a large number of virtual contexts easier.
	Increase number of global statements to 4K	The total number of global statements within the system is increased from 1K to 4K. This improves scalability when defining a pool of global addresses.
	Access list memory enhancements	Increase of 20% in total available access list memory. This improves scalability for access lists.
	Sessions for non-TCP/UDP packets	Non-TCP/UDP packets are forwarded through the fast path instead of the slow path. This improves performance for GRE, ESP, and multicast traffic.
	Support up to ten DHCP relay statements	Increases the number of DHCP relay statements from four to ten, which allows better scalability.
	80 HTTPS sessions for ASDM	Increases the current number of possible HTTPS sessions from 32 to 80 for ASDM.
Network Integration	Mixed L2 & L3 mode support	A mixture of L2 and L3 modes on the same FWSM is allowed, which enables flexible network deployments.
	Multiple pairs of L2 interfaces per context	The number of supported interfaces in transparent mode is increased from a single pair up to eight pairs pairs. This improves scalability and reusability of L2 contexts.
	Private VLAN support	FWSM is now aware of PVLANs configured on the Cisco Catalyst 6000 Supervisor and properly processes traffic coming from a secondary VLAN that is configured as a secure VLAN with 802.1Q tagging of the primary. This leverages the logical separation and traffic isolation provided by PVLANs.
	Per interface DHCP relay	Allows DHCP relay (helper addresses) to be configured for each interface rather than for the entire context. This allows better granularity and control of DHCP services.
Core IP Enhancements	IPv6 Phase 1	Support for inspection, security checks on headers, access lists, routing, and management to the device for IPv6 traffic. This supports the expanded addressing capabilities and native security offered by IPv6.
	Multicast support	Support for PIM-SM version 2 (RFC2362) dynamic routing as well as IGMP v2. This provides secure integration in distributed video conferencing and collaborative computing environments and reliable delivery of sensitive real-time streaming updates.
	dNAT for multicast	Destination NAT on the group addresses after packets are replicated protects internal resources from an external multicast source.
	OSPF neighbor	Allows FWSM to push OSPF routes over a VPN tunnel by statically defining neighbors and exchanging databases using unicasts. OSPF hello updates and OSPF adjacencies can be established over VPN tunnels.

Table 2 FWSM 3.1 Enhancements (continued)

Type of Feature	Feature	Description/Benefits
Monitoring and Management	SSHv2	SSHv2 provides a more secure way of accessing FWSM and improves security for management connections.
	Ping, logging and memory management enhancements	Extended ping, logging of subsystem identification when packets are dropped or discarded, enhanced messages for memory depletion conditions, user-configurable system message buffer size, and sanity checks for detecting memory corruptions.
	Syslog server failure policy for TCP transport	The FWSM can be configured to stop or continue processing if the syslog server fails when using TCP as the syslog transport.
	4K+ certificate support	The FWSM can work with certain certificate authorities for administrator authentication by supporting 4K key sizes. For example, Microsoft CA defaults to 4K Key sizes.
	SNMPv2c	SNMPv2C agent supports new features, such as 64-bit counters, enhanced MIBS (SNMPv2 MIB [RFC 1907], and the IF-MIB [RFC 1573,2233]). Provides uniform SNMP agent/MIB support with Cisco PIX Firewall and VPN3000.
	Additional MIBs	Includes other MIBs currently available on Cisco PIX Firewall and VPN3000 platforms. New additions are: CISCO-CRYPTO-ACCELERATOR-MIB.my, IF-MIB.my, CISCO-FIREWALL-MIB.my, CISCO-PROCESS-MIB.my, CISCO-SYSLOG-MIB.my, CISCO-REMOTE-ACCESS-MONITOR-MIB.my,CISCO-IPSEC-FLOW-MONITOR-MIB.my, ENTITY-MIB.my. This provides uniform SNMP agent/MIB support with Cisco PIX Firewall and VPN3000.
	Enhanced parser and CLI	FWSM CLI is enhanced by porting the Cisco IOS software parser and by providing functions such as command alias, comments in configuration file, command completion, command syntax check, and context sensitive help.
	Out of band management	Restricts management traffic to a specific interface. Enhances security for management connections.
	Prompt slot/status reporting	CLI enables/disables reporting the slot number and failover status as part of the FWSM session prompt. Identifies the slot in which the FWSM is installed and the failover status of the module.
	Debug message timestamp	Adds a timestamp for debugging messages. This improves ease of use for logged debug messages.
	System context logging to external syslog server	The system context can send logs to an external syslog server. This provides logging messages from the system context.
	Include ACE info as part of message 106023	The specific ACE entry is identified in the message, rather than just the access list name. This helps isolate traffic issues.

Software License Information

The FWSM supports the following licensed features:

- Multiple security contexts. The FWSM supports two virtual contexts plus one admin context for a total of three security contexts without a license. For more than three contexts, obtain one of the following licenses:
  - 20
  - 50
  - 100
  - 250
- GTP/GPRS support.

Limitations and Restrictions

See the following limitations and restrictions on the FWSM:

- Multiple context mode does not support dynamic routing protocols such as RIP and OSPF. Use static routing instead.
- Transparent firewall mode supports a maximum of eight interface pairs per context.
- For transparent firewall mode, you must configure a management IP address per interface pair.
- The outbound connections (from a higher security interface to a lower security interface) from an interface that is shared between the contexts can only be classified and directed through the correct context if you configure a static translation for the destination IP address. This limitation makes cascading contexts unsupported, because configuring the static translations for all the outside hosts is not feasible.
- The CPU-intensive commands, such as **copy running-config startup-config** (the same as the **write memory** command), might affect system performance, including reducing the successful rate of inspection and AAA connections. When a CPU-intensive action completes, the FWSM might produce a burst of traffic to catch up. If you limit the resource rates for a context, the burst might unexpectedly reach the maximum rate. We recommend using these commands during low traffic periods. Other CPU-intensive actions include the **show arp** command, polling the FWSM with SNMP, loading a large configuration, and compiling a large access list.

Open Caveats in Software Release 3.1(3)

This section contains open caveats in software release 3.1(3).

- CSCeh82940

  The **show mroute count** output displays incorrect values when multicast packets are forwarded by the FWSM.

  Workaround: None

- CSCei56437

  When using Bidirectional PIM multicast routing, the CPU usage is high when the FWSM is placed between the source DR and the RP.

  Workaround: None

- CSCei85820

  When multicast routing is enabled and multicast packets are forwarded by the FWSM, forwarding statistics shown with the **show mfib** command are incorrect.

  Workaround: None

- CSCsc76656

  In the **show conn** command output, the connection counter for "in most used" is incorrect. This happens when the FWSM is configured with a **url-server** with a large number of TCP connections. For example, **url-server (inside) host 100.0.0.0 pro tcp conn 50**.

  Workaround: None

- CSCsc79540

  Even if the Sun RPC inspection is enabled, and the pinholes are opened as shown by the **show sunrpc-server active** command, NIS+ logins still fail.

  Workaround: None

- CSCsc85246

  When the number of mfib entries have exceeded the maximum limit space available (5000 mfib entries), the mfib database fails to update the mfib entries. The FWSM fails to remove the mfib entries even after issuing the **clear pim topology** command.

  Workaround: Disable and then reenable multicast routing.

- CSCsc88494

  When the configured connection limit (**set connection conn-max**) is exceeded, the port number shown in system message 201011 is shown in network-byte-order, not host-byte-order. For example, the following system message has the port number as shown:

  ```
  %FWSM-3-201011: Connection limit exceeded 50/50 for inbound packet from x.x.x.x/260 to
  y.y.y.y/17664 on interface outside
  ```

  The real port numbers are 1040 and 69.

  Workaround: Convert the port numbers using the following calculation:

  a. Convert the system message port number to hexadecimal. For example:

     260 is 0x0104 in hexadecimal.

  b. Flip the hexadecimal bytes. For example:

     0x0104 flipped is 0x0410

c. Convert the flipped hexadecimal number to decimal. For example:

   0x0410 is 1040 in decimal.

- CSCsc95695

  If an HTTP request or response packet with an invalid minor version string passes through the FWSM, the FWSM fails to log or deny the packet.

  Workaround: None

- CSCsd08146

  In multiple context mode with each context assigned to a failover group (**join-failover-group**) for Active/Active failover, if you disable failover in the system configuration (**no failover**) at startup, then the FWSM drops traffic.

  Workaround: Remove the **join-failover-group** command from each context in the system configuration, or enable failover.

- CSCsd35168

  In manual commit mode, if you repeatedly clear an access list, you cannot add additional ACEs to the access list and it remains empty. For example, if you enter **clear configure access-list** *name*, then add an ACE, then clear it again, then you cannot add another ACE to the access list. You see the following error:

  ```
  ERROR: Unable to add, access-list config limit reached
  ```

  Now, if you commit the access list, it will be removed along with any associated **access-group** commands.

  Workaround: None

- CSCsd35194

  If you commit a very large access list (approximately 74 K rules) either automatically or manually, the FWSM takes approximately 2 hours to commit it, and you see a fatal error message even though it successfully committed:

  ```
  **** FATAL ERROR: Access Rule Download Failed ****
  ```

  The traffic does not pass through the FWSM before and after receiving the fatal error.

  Workaround: None

- CSCsd99448

  The **show conn detail** command shows the letter R for two different explanations:

  - R - outside acknowledged FIN
  - R - UDP SUNRPC

For example:

```
FWSM/6/sec/mtfw1/act(config)# sh conn detail
624 in use, 16954 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, k - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
 Network Processor 1 connections
```

Workaround: None

- CSCse05983

  After running into caveat CSCse01998 (the **no firewall module** *x* **vlan-group** *y* command on the switch removes all VLANs from the FWSM), the **show vlan** command on the FWSM does not show any VLANs, and the **interface vlan** command shows each VLAN in a down/down state. The **show idb** command shows the VLANs in an up/up state, and traffic passes through the FWSM. This problem is seen only with some combinations of VLANs.

  Workaround: When using a cascade image on the supervisor engine, this problem is not seen.

- CSCse07315

  After removing a secondary VLAN from a firewall VLAN group on the switch, and then adding the VLAN to another group, the first VLAN group cannot be added to the FWSM, and a warning message such as the following appears:

  ```
  Secondary vlan 339 can't be configured as secure for module 9. Command rejected.
  ```

  Workaround: None

- CSCse38548

  When a **static** command is configured with a network mask, and an inbound ICMP packet is sent to the network IP address, the FWSM builds a static translation instead of generating syslog message 305006.

  Workaround: None

- CSCse18085

  If an existing BVI interface is remove and then re-added, the interface status shown by the **show interface bvi** command is seen as “administratively down” with a protocol status of “up” instead of the actual “up” and “up” status. The **show interface ip brief** command shows the status as “administratively down” with a protocol status of “down” instead of the actual “up” and “up” status.

  The functionality of the interface is not affected.

  Workaround: Use a bridge group number other than one which was removed. The interface status shows correctly after you reload the FWSM.

- CSCse49319

  Communication between the inside and outside interfaces of a context fails after adding the below two commands to the system configuration that does not yet have any other **failover** commands:

  ```
  failover group n
  context xxxx
     join failover group n
  ```

Workaround: Configure the below minimum **failover** commands:

```
failover lan unit primary
failover lan interface name vlannumber
failover interface ip name ipaddress mask standby ipaddress
failover
```

- CSCse52679

  The FWSM might crash unexpectedly in Thread Name: SNMP.

  Workaround: None

- CSCse53555

  After adding and removing an ActiveX or Java filter for any port, the original filter stops working.

  Workaround: Enter the **clear configure filter** command, and then reconfigure the filter.

- CSCse54221

  The **limit-resource all** command cannot be configured. This can lead to one context hogging the CPU and causing connectivity problems during the implementation of changes.

  Workaround: None

- CSCse57634

  If you upgraded to Version 3.1, then the **snmp-server listen-port** command in the startup configuration in multiple context mode might cause the FWSM to crash if traffic is present when the FWSM boots.

  Workaround: Boot into the maintenance partition and remove the startup configuration. Remove the **snmp-server listen-port** command from the startup configuration before copying it back to the FWSM.

- CSCse58933

  Using a large number (10 K) of time range ACEs may cause the system to become unstable and crash.

  Workaround: None

- CSCse59188

  When a time range is used in an ACE with an object-group, the **show time-range** command does not show “used in: IP ACL entry”.

  Workaround: None

- CSCse59206

  When a time range applied to an ACE with an object-group becomes inactive, the ACE is still active and traffic passes through.

  Workaround: None

- CSCse60868

  With Active/Active failover, if you have an explicit **access list deny ip any any** ACE at the end of an access list that also contains an ACE with an object group, then the access list blocks all traffic, including traffic that you permitted.

  Workaround: Configure all the object groups before you apply the access list to interfaces; add the explicit **access list deny ip any any** ACE to the access list after you apply the access list to the interfaces. Do not modify the access list in the standby context.

Alternatively, do not use an explicit **access list deny ip any any** ACE; there is an implicit **deny ip any any** at the end of every access list.

- CSCse63602

  The FWSM changes the UDP checksum on non-NAT interfaces when the RP router is set downstream with respect to the FWSM.

  Workaround: Use the **nat** command instead of the **static** command, or move the RP router upstream.

- CSCse64078

  The FWSM might experience a memory leak after running traffic for 72 hours. You see the following error message:

  ```
  ERROR: Failed to allocate memory for show Conn request
  ```

  Workaround: None

- CSCse64571

  When you enter the **show pim topology** command, there are no interfaces in olist shown for the (S,G) entry.

  Workaround: Enter the **show mfib** command to view the list of out interfaces for a given (S,G) entry.

- CSCse65207

  In multiple mode, the FWSM shows the maximum interfaces as 300 in the **show version** output, instead of the correct 1000.

  Workaround: None

- CSCse66244

  When enabling URL filtering in multiple context mode, URL lookup requests are sent to the filtering server. Under certain circumstances, the FWSM delays these filtering requests so that web access performance is diminished.

  Workaround: Disable URL filtering to restore regular web access performance.

- CSCse66612

  When the FWSM is configured with a chain limit using the **fragment chain** command and traffic is sent with large size data, the FWSM should show the message "Discard IP fragment set with more than *n* elements", but the logs shows an incorrect value.

  Workaround: None

- CSCse66943

  FWSM logs are not generated when tiny IP fragments are sent.

  Workaround: None

- CSCse68170

  When the FWSM is configured to send system log messages to a mail server, the connection is created, but the logs are not sent.

  Workaround: None

- CSCse68777

  If the FWSM in failover ends up in pseudo-standby mode, it uses its own MAC address with active IP addresses; in which case, there will be two units using the same IP addresses.

Workaround: None

- CSCse68890

  The FWSM reloads when a service policy configured for inspecting FTP, TFTP, and HTTP (but not ICMP) is applied to an interface containing a class map that matches a large access list containing 10 K ACEs.

  The FWSM reloads only if a new service policy is applied in addition to the default service policy, global_policy, which is applied globally to all interfaces by default.

  The FWSM might reload on the first attempt when a service policy is applied to an interface. Sometimes on the first attempt, it gives the below error message:

  ```
  hostname(config)# service-policy abc interface inside21
  ERROR: Unable to add, fixup config limit reached
  ERROR: cannot add policy to rule engine
  ```

  Workaround: Remove the default global_policy before applying the new service policy that uses the large access list.

- CSCse69719

  In doing a snmpwalk on the FWSM, the ifOutOctets MIB shows incorrect numbers

  Workaround: None

- CSCse70408

  UDP packets with a source port equal to zero will be dropped by the FWSM when you specify the destination port in the interface access list.

  For example, the following access list allows any UDP source port but specifies the destination port of 53; the system log message shows that the packet was dropped:

  ```
  hostname(config)# access-list inside extended permit udp any any eq 53

  %FWSM-4-106023: Deny udp src inside:x.x.x.x/0 dst outside:y.y.y.y/53 by access-group
  "inside" [0x0, 0x0]
  ```

  Workaround: Remove the destination port number in the access list and restrict access based only on protocol and IP addresses.

Resolved Caveats in Software Release 3.1(3)

- CSCse63843

  Packet loss is experienced when a large packet needs to be fragmented by the FWSM on its way out.

  Workaround: Increase the MTU size on the outgoing interface of the FWSM. For example, if the packet size is 5K, change the MTU size on the outgoing interface of the FWSM to a larger value, like 8K. Use the **mtu** *interface_name bytes* command to change the MTU size.

Resolved Caveats in Software Release 3.1(2)

- CSCsd13952

  In multiple transparent mode, if you configure a syslog server with the **no logging permit-hostdown** command, the FWSM fails to drop the traffic when the syslog server is unreachable.

  Workaround: None

- CSCsd15128

  When using Active/Active failover, if you remove an interface from a security context that is shared with other contexts (or remove the security context with a shared interface), then traffic on that VLAN might be dropped, even though the VLAN is still in use in other contexts.

  Workaround: None

- CSCsd22574

  If you enter the **clear configure static** command, and the **static** command was configured with the **interface** keyword, then the real interface IP address can be pinged from the supervisor engine. After failover, however, the real IP address cannot be pinged from the supervisor engine.

  Workaround: Reconfigure the IP address on the interface.

- CSCsd29170

  If you enter the **show np 2 vlan 4096** command on the FWSM, it crashes.

  Workaround: None. Other VLAN values do not crash the FWSM.

- CSCsd30940

  If you use SIP IP Address Privacy in conjunction with PAT, then the FWSM fails to allow media traffic. The two inside phones register with the outside proxy, but the FWSM drops media connections.

  Workaround: Use dynamic NAT instead of PAT with SIP Address Privacy.

- CSCsd31483

  If you modify the SIP inspection configuration, RTP traffic cannot pass through the FWSM.

  Workaround: Use the default inspection policy.

- CSCsd32211

  In multiple transparent mode, if you enter the **show asp table mac-address-table** command in the system execution space, the FWSM crashes.

  Workaround: None

- CSCsd33022

  Using an extended ping in the system execution space over an SSH connection to the admin context hangs the session and might crash the FWSM if the session is cleared.

  Workaround: Use Telnet to the admin context instead of SSH; or connect to the system execution space from the switch using the **session** command. You can also reduce the SSH timeout so that if it hangs, you do not have to manually clear it.

- CSCsd91062

  The FWSM might traceback with “Thread Name: Checkheaps” and “assertion “0” failed: file “malloc.c:, line 4578”.

  This occurs when a protocol using a port reserved for CTIQBE or H323 sends packets greater than 8192 bytes in size, with H323 or CTIQBE inspection enabled on the FWSM. The correct behavior is to create a system log message to indicate when the proxy buffer limit is reached during the reassembly process. When this happens for H323 and CTIQBE, the connection goes from proxy to non-proxy mode.

  Workaround: This could be normal in many cases. A packet capture would help narrow down the packets causing the reassembly limit to exceed.

- CSCsd97155

  In rare situations, an FWSM might crash and not complete the crash process. As a result, the FWSM might not reload during the crash process as normally expected.

  Workaround: There is no workaround at this time. The only option is to reload the FWSM if accessible by **session** or **ssh** or alternatively reset the FWSM from the CLI of the switch.

- CSCse04914

  The packet capture feature is only capturing ingress (inbound) packets, not egress (outbound) packets.

  Workaround: None

- CSCse17704

  Using outside policy NAT, all outside traffic requires NAT to pass through the FWSM even with NAT control disabled.

  Workaround: None

- CSCse23177

  If you modify a **global** command, and then enter the **clear xlate** command, no translations are reestablished and traffic does not flow through the FWSM.

  Workaround: Remove the current **global** command and re-add it.

Related Documentation

See the following sections for related documentation:

- Hardware Documents, page 17
- Software Documents, page 18

Hardware Documents

See the following related hardware documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation Note*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*

Software Documents

See the following related software documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*
- *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1*
- *Catalyst 6500 Series Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Cisco IOS Command Reference*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.