Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module Software Release 3.1(x)

February 2011

This document contains release information for FWSM releases 3.1(1) through 3.1(20).

This document includes the following sections:

Important Notes

- You must install maintenance software Release 2.1(2) before you upgrade to FWSM Release 3.1. See *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

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

features that are supported on the PIX and ASA platforms are not enabled for FWSM. You can disable the limited TCP normalization support for the FWSM using the **no control-point tcp-normalizer** command.

Upgrading the Software

See *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.

To upgrade between 3.1(x) maintenance releases, see the "Managing Software, Licenses, and Configurations" chapter in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

Note Due to CSCse74946, hitless upgrades using failover between 3.1(1) and other 3.1(x) maintenance releases are not supported. Only 3.1(1) is affected.

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(33)SRD6 (for the Cisco 7600 series router)	720-3C-1GE (No PISA integration, no Route Health Injection, no Virtual Switching system)
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	2, 720, 32
Cisco IOS Software Modularity	

Table 1 Support for FWSM 3.1 (continued)

	Supervisor Engines[1]
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(1).

Table 2 FWSM 3.1(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 a AAA server is not available.
	AAA server checks all TFTP commands for authorization	If command authorization is turned on, then all TFTP server commands are checked by the AAA server for authorization. If users are not authorized to use the command, then the request is denied. In previous releases, only the **configure net** command was checked for authorization. **Note** Note: If you have many access lists configured for your network, then this could result in a delay while the server is checking them.
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 an 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.

Table 2 FWSM 3.1(1) Enhancements (continued)

Type of Feature	Feature	Description/Benefits
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(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—Third Generation Partnership Project) 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 CallManager 4.0.

Table 2 FWSM 3.1(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(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 4 K	The total number of global statements within the system is increased from 1 K to 4 K. 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 (RFC 2362) 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(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.
	4 K+ certificate support	The FWSM can work with certain certificate authorities for administrator authentication by supporting 4 K key sizes. For example, Microsoft CA defaults to 4 K 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 security appliance and VPN 3000.
	Additional MIBs	Includes other MIBs currently available on the Cisco PIX security appliance and VPN 3000 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 security appliance and VPN 3000.
	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; however, when multiple bridge-group interfaces exist in a single context, inspection may not work properly. We recommend that you create a separate context for traffic that requires inspection.
- 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.
- When a large number of VLANs are configured to receive multicast streams, multicast traffic can be received on and forwarded from the first 100 VLANs configured on the FWSM, but VLANS beyond the first 100 might not forward multicast traffic.
- 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.
- If you try to save a new configuration file with the **write memory all** command in the system execution space, and there is not enough space on the disk, then the error “writing disk: message” displays; the new configuration is not saved, and the FWSM removes the existing old configuration file from the disk.

  Be sure to either:
  - Free some space from the disk.
  - Go to each context and issue the **write memory** command instead of saving all contexts from the system.

Open Caveats in Software Release 3.1

This section contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from later releases. For example, if you are running Release 3.1(4), then you need to add the caveats in this section to the resolved caveats from 3.1(5) and later to determine the complete list of open caveats.

- 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.

- 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.

- CSCse13916

  Windows Messenger Version 5.0 or 5.1 does not sign on with Live Communication Server 2003, Live Communication Server 2005, or any other SIP application that multiple SIP messages within the same packet; the packets are dropped. Cisco IP Phones that run SIP are not affected by this caveat.

  Workaround: Configure your SIP applications to send smaller SIP messages, or increase the MTU on the FWSM interface using the **mtu** command if it was previously configured with a smaller than default MTU. The default MTU is 1500 bytes.

- CSCse56960

  With bidirectional PIM, if the router that is configured as the RP is directly connected to the FWSM, no joins are sent to the RP by the FWSM. The debug logs show the following error message: “NO RPF NEIGHBOR o send J/P.” The **show mroute** and **show mfib** commands display correct flags and RPF neighbors.

  Workaround: Do not make the directly-connected router the RP.

- CSCsg75173

  URL filtering with Websense causes high CPU in high traffic loads.

  Workaround: None.

- CSCsi73738

  High CPU is seen when a client accesses an ISEE server (sPOP) and HTTP inspection is enabled.

  Workaround: Disable the tcp normalizer using the **no control-point tcp-normalizer** command or disable HTTP inspection.

- CSCsk01370

  The FWSM is not forwarding all DNS requests from the outside interface to the inside interface when the **inspect dns max-length** command is used.

  Workaround: Disable the **inspect dns max-length** command.

- CSCsk35549

  Connections that have their TCP state bypassed (using the **set connection advanced-options tcp-state-bypass** command) generate SYN Timeout syslog messages when they idle out. The TCP SYN packets do indeed pass through the FWSM, but the syslog message indicates the tear down reason as a SYN timeout.

  For example:

  ```
  Teardown TCP connection 13223832 for outside:10.10.10.100/1304 to
  inside:192.168.1.100/1234 duration 2:02:53 bytes 7798136 SYN Timeout
  ```

  Also the connection flags for a connection with its TCP state bypassed indicate one of the following groups of flags:

  ```
  bBs - (b)State bypass, (B)initial SYN from outside, (s)awaiting outside SYN
  bBS - (b)State bypass, (B)initial SYN from outside, (s)awaiting inside SYN
  bs  - (b)State bypass, (s)awaiting outside SYN
  bS  - (b)State bypass, (s)awaiting inside SYN
  ```

  Because the FWSM is not tracking the state of the connection, flags indicating the direction of traffic and whether or not correct SYN packets were received, may be inconsistent and misleading.

  Workaround: None.

- CSCsk61834

  Directed BOOTP messages are redirected to a DHCP server if DHCP Relay is enabled on the FWSM and DHCP Relay servers are configured.

  Workaround: None.

- CSCsl10122

  The primary and secondary FWSMs might crash in Thread name: snmp. This is caused when there is no proper response from the NP due to high traffic. Also there is no **snmp-server host** command configured in the system but in the configuration, there is the **snmp-server enable traps snmp authentication linkup linkdown coldstart** command.

  Workaround: Remove the **snmp-server traps** command.

- CSCsm46399

  In single mode, using FTP with **inspect ftp** enabled results in a 10% drop in connections per second handled by the FWSM. Once a connection is established, data traffic does not experience any drop.

  Workaround: None.

- CSCsm73157

  Failover is not working on the FWSM in transparent mode. When connectivity is broken on one or two interfaces, The FWSM is not updating the MAC address with the updated path. Therefore, users are losing their connections.

  Workaround: None.

- CSCso38838

  In rare circumstances, traffic matching a static policy NAT statement may fail with a “no translation group found” syslog message even though it matches the policy access list.

  Workaround: Try redefining the policy access list with a different access list name and applying that to the **static**.

- CSCsv50778

Outside policy PAT in multiple context mode uses an inactive access list to create xlates after the memory partition of the context is changed using the **allocate acl-partition** command.

Workaround: Reconfigure the access list and policy PAT after changing the memory partition.

- CSCsv71697

  When outside policy PAT is configured and traffic is sent from outside to inside host, then xlates on a standby unit have incorrect flags of Identity (I) instead of portmap (r) and shows the xlate as NAT instead of PAT.

  Workaround: None.

- CSCta73803

  The FWSM in multiple context mode might experience a depletion in the 16384 byte blocks if multiple contexts are subjected to SNMP polling simultaneously. Once in this condition, the FWSM must be rebooted to recover.

  To detect if the FWSM is in this state, enter **show blocks** and look for the line starting with "Slow Path". If the CNT column is at 0 and stays at 0, this issue might be the cause.

  For example:

```
FWSM# show blocks
  SIZE    MAX    LOW    CNT
     4   1800   1790   1800
    80   1000    976    983
   256   1600   1529   1586
  1550  11575  10483  11540
  2048   1384   1349   1383
 16384   8192   2181   2182

Additional Block pools for 16384 size blocks
 IP Stack 1024  1023   1024
ARP Stack  512   510    512
Slow Path 5500     0      0     <--- Problem here
    NP-CP 1024  1017   1024
   Others  132   132    132
```

  Additionally, the output of **show blocks old | begin 16384** will show output relating to SNMP.

  For example:

```
FWSM# show blocks old | b 16384
Class 8, size 16384
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x0a7f0aa0  0x00411557  0x00a30608         44         101           0   put
udp_usr_input/ifc:65535/snmp
0x0a7ec780  0x00411557  0x00a30608         39         123           0   put
udp_usr_input/ifc:65535/snmp
0x0a7e8460  0x00411557  0x00a30608         39         132           0   put
udp_usr_input/ifc:65535/snmp
0x0a7e4140  0x00411557  0x00a30608         39         128           0   put
udp_usr_input/ifc:65535/snmp
0x0a7dfe20  0x00411557  0x00a30608         39          85           0   put
udp_usr_input/ifc:65535/snmp
0x0a7dbb00  0x00411557  0x00a30608         44         100           0   put
udp_usr_input/ifc:65535/snmp
0x0a7d77e0  0x00411557  0x0041dcc5         39         123           0   put
udp_usr_input/ifc:65535/snmp
...
```

  Workaround: Configure the SNMP management server to not query the following OIDs:

- TCP Connections—1.3.6.1.2.1.6.19.1.

- UDP Connections—1.3.6.1.2.1.7.7.1.
- Translation tables—1.3.6.1.2.1.123.1.8.1.1.

Resolved Caveats

This section lists the resolved caveats for each maintenance release and includes the following topics:

Resolved Caveats in Software Release 3.1(20)

The following caveats were resolved in Release 3.1(20) and were not previously documented. If you are a registered Cisco.com user, you can view more information about the caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/

- CSCtk61424 — OpenSSL Ciphersuite Downgrade and J-PAKE Issues

  Symptom:

  The device may be affected by an OpenSSL vulnerabilities described in CVE-2010-4180 and CVE-2010-4252.

  Conditions:

  Device configured with any feature that uses SSL.

  Workaround:

Not available

PSIRT Evaluation:

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.1/3.8:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:U/RC:C

CVE IDs CVE-2010-4180 and CVE-2010-4252 have been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCtl21186 — Cmd authorization fails for certain commands on fallback to LOCAL db

  Symptom:

  Certain commands like 'show running-config', 'show interface' are allowed to be executed by users with lower privilege-level when fallback has occured.

  Conditions:

  1. Fallback to LOCAL is configured

  2. All FWSM commands are assigned their default privilege levels in LOCAL db.

  3. Users with lower privilege-level than 15 login into privileged-exec mode and execute 'show running-config' or 'show interface' commands, and some config commands.

  Workaround:

  none.

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2

  score. The Base and Temporal CVSS scores as of the time of evaluation are 6.0/5.0:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C

  CVE ID CSCtl94142 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can befound at the following URL:

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

- CSCtl84952 — SCCP inspection DoS vulnerability

  A vulnerability exists in the Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers that may cause the Cisco FWSM to reload after processing a malformed Skinny Client Control Protocol (SCCP) message. Devices are affected when SCCP inspection is enabled.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-fwsm

  Note: Cisco ASA 5500 Series Adaptive Security Appliances are affected by the vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose this and other vulnerabilities that affect the Cisco ASA 5500 Series Adaptive Security Appliances. The advisory is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-asa

Resolved Caveats in Software Release 3.1(19)

The following caveats were resolved in Release 3.1(19) and were not previously documented. If you are a registered Cisco.com user, you can view more information about the caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/

Table 3 Resolved Caveats in Release 3.1(19)

Caveat	Description
CSCtf57135	FWSM 3.2 - deny-flow-max stuck when denied is not at 4096
CSCtj21761	term pager command affects all sessions and future sessions

Resolved Caveats in Software Release 3.1(18)

The following caveat was resolved in Release 3.1(18), and was not previously documented. If you are a registered Cisco.com user, view more information about the caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

- CSCte49110 : FWSM setting DF bit on reassembled skinny packet

Resolved Caveats in Software Release 3.1(17)

The caveats in Table 4 were resolved in Release 3.1(17), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 4 Caveats Resolved in Release 3.1(17)

Caveat ID	Title
CSCsx97979	ENH show np x thread - should display all thread output
CSCsz50233	Dev: NP Hard assert in Move_TFTP_Emb
CSCta60764	Cut-thru-proxy:certificate error after completion of intial authenticati
CSCtb18847	NP 3 pause indefinitely with established command
CSCtb76719	Meaning of Flags 's' and 'S' is Reversed in 'show conn detail' Output
CSCtb88893	Transparent mode FWSM , Active passing braodcast arp from standby
CSCtc36651	FTP fails in Active/Active mode when two contexts not active on same FW
CSCtc40207	Standby transparent FWSM might send arp request using active MAC
CSCtd04061	IMPORTANT TLS/SSL SECURITY UPDATE

Resolved Caveats in Software Release 3.1(16)

- CSCsz51960

  In failover, the standby FWSM becomes unresponsive with Thread Name: fover_ifc_test.

  Workaround: None.

The caveats in Table 5 were resolved in Release 3.1(16), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 5 Caveats Resolved in Release 3.1(16)

Caveat ID	Title
CSCsz57041	Inconsistent behavior in adding access-list remark in manual-commit mode
CSCsz66958	FWSM should send gratuitous ARP if new Primary inserted in failover
CSCsz68425	Transparent FWSM not Sync'ing Valid CAM Table Entries to Failover Peer
CSCsz97207	NP 2 threads lock due to processing malformed IP packet
CSCta08654	Intface in shut down status intercepts traversing traffic
CSCta10823	In certain case ACE limit reached error is not appearing in Manual mode

Resolved Caveats in Software Release 3.1(15)

- CSCsl63063

  The FWSM might unexpectedly stop passing traffic and reload. The output of the **show crash** command shows a traceback in thread "doorbell_poll". The NP Hard Debu in the NP Hard Assert Info (included in the **show crash** output shows a crash in processor NP1 or NP2 at PC 0x3a1a.

  Workaround: None.

The caveats in Table 6 were resolved in Release 3.1(15), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 6 Caveats Resolved in Release 3.1(15)

Caveat ID	Title
CSCsl68060	Traceback in Thread Name: OSPF Router
CSCsm96999	Saving a config to disk:,"sh disk:" and "dir" gives diff saved times
CSCsr68825	Failover: FWSM should not send TCP RST unless it is Active
CSCsu21962	FWSM unexpectedly reloads in Thread Name: doorbell_poll or Syslog_entry
CSCsv14944	FWSM unexpectedly reloads at Thread Name: doorbell_poll 0x3cec NP1 / NP2
CSCsv42245	HTTP traffic not going through with routed ASR topology
CSCsv46585	Modifying an ACL can cause traffic to be incorrectly allowed
CSCsv82747	Portmap translation problems after failover

Table 6 Caveats Resolved in Release 3.1(15) (continued)

Caveat ID	Title
CSCsw77676	FWSM: No logging message 710003 does not work
CSCsw79372	Fwsm 3.2 might stop processing incoming ospf hellos on some interfaces
CSCsx08762	ENH: Established entries in CP and NP go out of sync for sunrpc traffic
CSCsx09390	VSS: After redudancy force-sw, session to secondary fwsm is faling.
CSCsx15526	Capture command shows all tcp flags set for inspected traffic
CSCsx34429	NAME command on FWSM doesn't accept 128.0.0.0 and 192.0.0.0 as a network
CSCsx59229	Standalone 'Failover' Command Stops All Local Outgoing Traffic
CSCsx75701	FWSM log 106101 triggered but max flows not reached
CSCsx82996	Traceback: doorbell_name
CSCsy00911	Abnormal Consumption of 56 and 80 Byte Memory Segments with Logging Mail
CSCsz47735	FWSM doesn't support H323 with VCON MXM 4.7 and XPoint 7.500.062

Resolved Caveats in Software Release 3.1(14)

The caveats in Table 7 were resolved in Release 3.1(14), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 7 Caveats Resolved in Release 3.1(14)

Caveat ID	Title
CSCsv27205	FWSM - access-group are bypassed if source address is Class E
CSCsv49613	FWSM, TCP Checksum Error on certain packets
CSCsv83322	FWSM 'Who' Command is Locked in Configuration Mode
CSCsv99839	H323 packets dropped with new VCON MXM and XPoint client SW
CSCsw17796	FWSM access-group is not automatically updated for an ipv6 access-list
CSCsw39406	rsh inspection uses wrong xlate for pinhole
CSCsx08762	ENH: Established entries in CP and NP go out of sync for sunrpc traffic

Resolved Caveats in Software Release 3.1(13)

- CSCsu43711

  The FWSM reloads when a Cisco ASA 5500 series adaptive security appliance is configured as its failover peer and placed on the respective failover control VLAN.

  Workaround: Disallow the FWSM failover control VLAN on all trunks and access ports of the switch, or configure a failover key.

The caveats in Table 8 were resolved in Release 3.1(13), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 8 Caveats Resolved in Release 3.1(13)

Caveat ID	Title
CSCsf03695	Crash while creating captures for FWSM
CSCsi54863	FWSM: new MPC command to clear TCP Sack-Permitted option in 3WHS - SACK
CSCsm90200	Show memory displays incorrect data in multi context mode
CSCsq61452	Multicontext FWSM pair has continual reload with no crashinfo written
CSCsr47554	AAA Authentication request packet for 'show running-config' corrupted
CSCsr83767	Clear route permanently removes static routes from the NP 3
CSCsu01813	FWSM 3.2: redirected sqlnet data connections should not be inspected
CSCsu02947	FWSM: Traceback in Thread Name fast_fixup
CSCsu83857	console hung after "access-list commit" in 3.2.8 and 4.0
CSCsu85193	FWSM - policy nat rules are not replicated to standby
CSCsv19445	FWSM may not program routes into NP3 upon bootup.
CSCsv21077	FWSM traceback in fast_fixup

Resolved Caveats in Software Release 3.1(12)

- CSCsj48421

  If you have two dynamic policy NAT commands, and traffic matches the access list in one of the NAT commands; then you change the access list in the other NAT command so there is an overlapping ACE that also matches the same traffic; then no NAT entries are created for that traffic.

  Workaround: Remove and reapply the unchanged NAT statement (the NAT statement that was formerly used to match the traffic). This change forces the other NAT pool (with the updated access list) to take effect.

- CSCsm99224

  If you have overlapping **static** commands that both match the same traffic, and you add an ACE using the **line** keyword to an access list being used by the higher priority **static** command, then any traffic that should use the higher priority **static** command now uses the lower priority **static** command.

  Workaround: Remove and readd the **static** command after you alter the access list.

- CSCsq90172

  The FWSM may experience a failover event or stop responding completely after an extensive series of ICMP Echo Request packets is generated either to the FWSM or from the FWSM command line interface.

  Workaround: None.

- CSCsq87373

In multiple context mode with Failover, the secondary FWSM might crash after you commit configuration changes on the primary unit. After the crash, reloading the secondary FWSM causes it to enter Failover Off (pseudo-Standby) state. Both units have to be reloaded to re-establish the failover pair.

Workaround: None.

- CSCsq79074

  The Maximum Segment Size (MSS) option in the TCP header in the SYN ACK segment is passed unchanged when traversing the FWSM, regardless of what is configured with the **sysopt connection tcpmss** command. The MSS option on the initial TCP SYN segment is adjusted correctly. This occurs when the TCP options length is small (8 bytes or so).

  Workaround: None.

The caveats in Table 9 were resolved in Release 3.1(12), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 9 Caveats Resolved in Release 3.1(12)

Caveat ID	Title
CSCso02252	Overlapping networks dont translate DNS address in 3.1.x
CSCso25009	FWSM 3.2 : Capture on the egress interface may show corrupt packets
CSCsq16078	Various Stateful Failover failures in FWSM 3.1.10
CSCsq61452	Multicontext FWSM pair has continual reload with no crashinfo written
CSCsq66164	106101: Number of cached deny-flows for ACL log generated incorrectly
CSCsq75892	assert at ibm_4gs3_ingress:ibm_4gs3_dispatch_pkt+1204
CSCsq84306	SQLnet inspection overwrites HOST field in the redirect packet
CSCsq87373	In Multicontext Mode Secondary FWSM crashes when commiting configuration
CSCsr05764	FWSM blocks traffic due to route mismatch in CP and NP, NIC underruns
CSCsr21268	FWSM crashed at time_range.c after enabling failover
CSCsr29124	PAT src port allocation policy negates effect of host port alloc. policy
CSCsr40970	Strict HTTP inspection - problems with out-of-order packets from server
CSCsr45802	FWSM fails over when compiling ACLs if CPU also busy inspecting traffic
CSCsr51684	ERROR: np_logger_query request .Traffic failing on FWSM
CSCsr60593	FWSM: May crash in Thread Name: accept/http
CSCsr62662	FWSM may crash during 'fsck disk:' operations
CSCsr75501	FOVER:Standby MAC addr is improperly registered as Active MAC on Primary
CSCsr93090	High CPU on FWSM due to AAA accounting/authentication

Resolved Caveats in Software Release 3.1(11)

- CSCsm69869

The syslog message 305005 (No translation group found for...) should be generated for packets dropped due to a missing outside NAT exemption rule, but it is not. When outside NAT is configured along with **nat-control** enabled, all traffic not included in the outside NAT configuration must be included in an outside NAT exemption rule. If not, it is the expected behavior that these packets are dropped.

Workaround: None.

- CSCsk98142

  The FWSM might unexpectedly stop passing traffic and reload. The output of the **show crash** command shows a traceback in thread "doorbell_poll". The NP Hard Debu in the NP Hard Assert Info (included in the **show crash** output shows a crash in processor NP1 or NP2 at PC 0x59c2.

  Workaround: None.

The caveats in Table 10 were resolved in Release 3.1(11), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 10 Caveats Resolved in Release 3.1(11)

Caveat ID	Title
CSCso22765	Configuring overlap nat causes FWSM throws an error and discards config
CSCso35706	sysopt np completion-unit status not correct in Multicontext mode
CSCso63107	"Unable to add, fixup config limit reached" when class-map has match ACL
CSCso65731	"write mem" from HTTPS adds no monitor-interface CLIs to startup config
CSCso65918	DNS guard does not close DNS connections in cascaded context
CSCso69586	FWSM failover pair with vlan mismatch may go active/active
CSCso75761	portmap_index: unable to locate fixup appears when ACL is modified
CSCso95053	FWSM may report syslogs with very high port numbers
CSCsq09303	FWSM 3.1: allocate-acl-partition command makes inactive ACE active
CSCsq09883	AAA shell command set fails for some commands
CSCsq19327	FWSM drops ftp "Response: 125" after transfering 900+ files
CSCsq27152	ASDM location commands do not appear in show run all output
CSCsq34834	traceback in thread snmp during configuration replication
CSCsq43713	WIth FWSM code 3.2(5) one of the FWSM goes in failed state (DDTS is still in A state)
CSCsq55738	Addresses used in Static NAT are no longer advertised in OSPF
CSCsr14332	FWSM may calculate ACL line numbers incorrectly in manual commit mode

Resolved Caveats in Software Release 3.1(10)

- CSCsi27512

  The FTP client/server does not close a connection in some cases when the server uses a multiline 221 closure sequence:

  ```
  221-You have transferred 0 bytes in 0 files.
  ```

```
221-Total traffic for this session was 2551 bytes in 1 transfers.
221-Thank you for using the FTP service on orbi.
221 Goodbye.
```

instead of the classic sequence:

```
221 Goodbye;
```

Workaround: Disable FTP inspection or disable the 221 multiline closure sequence.

- CSCsk73347

  The FWSM logs syslog message #305006 ("<...> translation creation failed") even when sufficient NAT and/or PAT resources are available. This message occurs when the FWSM has a high NAT or PAT xlate reuse rate.

  Workaround: Increase the NAT and/or PAT pool or reload the FWSM to temporary clear the condition.

- CSCsk80400

  If you use an access list for static policy NAT and then insert an ACE in the access list; and the access list includes another ACE lower down (at a higher number) that can match the same traffic as the new ACE; then traffic that should match the new ACE because it is hit first instead matches the older ACE at the higher line number.

  Workaround: Finalize the access list configuration before attaching it to the static policy NAT command.

- CSCsl04546

  The FWSM might crash in Thread Name: websns_rcv_udp when Websense filtering is configured.

  Workaround: None.

- CSCsl05878

  The FWSM might crash when RIP is running. The crash shows: Thread Name: route_process (Old pc 0x00bbf8b6 ebp 0x0a5fe764)

  Workaround: None.

- CSCsm41796

  After failover, the **inspect ftp** feature does not work; the data channel is not opened on the first FTP connection attempt. However, the connection does go through on the second try.

  Workaround: Retry your FTP attempt, and the connection succeeds.

- CSCsm69810

  When configuring outside policy NAT in conjunction with outside NAT exemption, the policy NAT is never applied as configured. Even though the flow is excluded from the NAT exemption by configuring a deny ACE, a dynamic identity xlate is built for the outside source. All traffic is NAT exempted.

  For example:

```
global (inside) 5 10.10.10.50-10.10.10.60
nat (outside) 0 access-list nonat outside
nat (outside) 5 access-list nat outside

access-list nonat extended deny ip host 192.168.49.57 host 172.16.10.1
access-list nonat extended permit ip any any
access-list nat extended permit ip host 192.168.49.57 host 172.16.10.1
```

  192.168.49.57 should be translated to the global pool, but it is not.

Workaround: The outside NAT exemption is only required when the **nat-control** command is enabled. If you disable NAT control (**no nat-control**) then you can remove the outside NAT exemption command.

The caveats in Table 11 were resolved in Release 3.1(10), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 11 Caveats Resolved in Release 3.1(10)

Caveat ID	Title
CSCsm68082	Error: Bad Octal (digit > 7) may appear with MGCP inspect
CSCsm84230	Policy Nat stops working when ACE duplicated through obj-grp and deleted
CSCsm35626	FWSM 3.2.2 - conns per sec usage under asdm not accurate
CSCsm50370	ip address command breaks routing with duplicate statics
CSCsm58073	When saving a config to disk:/, the time is one day ahead
CSCsm87914	FWSM 3.2 crash in Thread Name: Logger
CSCsm42519	FWSM crashes in Thread Name: radius_snd
CSCso03094	Traceback in 'perfmon' thread
CSCso06060	Failover packet from FWSM has incorrect DSCP value
CSCso00289	Unable to Disable TCP Sequence Number Randomization
CSCso11666	No pim command will not replicate on standby unit
CSCso14069	FWSM is not processing "stop on error" correctly
CSCso17150	FWSM 'failover interface-policy' impact on transparent A/A configuration
CSCso33286	long AAA ACLs requires >1h compilation time.
CSCsm86434	FWSM user auth dialogue box not re-presented for longer period in 3.1.8
CSCso42729	Sunrpc sessions are not deleted from np 3 established list
CSCsl05878	FWSM reload with panic: route_process
CSCso71324	URL Filtering Traceback with Thread Name HTTP
CSCsm53140	Inconsistancy in sysopt tcp window-scale configuration

Resolved Caveats in Software Release 3.1(9)

- 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.

- CSCsh62757

The wrong TLV parameters are received by the FP when a TLV update has a wrong field (the function ID is out of the range). This situation causes the FP to assert and generate a crash (door_bell pool).

Workaround: None.

- CSCsj04022

  When the last batch of commands committed includes inspection rules, and the new rules caused memory exhaustion, then the new rules are not automatically removed from the configuration even though they exceed the rule limit causing other rules not to load correctly.

  Workaround: Remove the last batch of inspection rules from the current configuration.

- CSCsl00215

  When both the client and the server agreed with the use of the TCP window scale option, then the FWSM:

  a. Does override the MSS of the client (in the first SYN).
  b. But does *not* override the MSS of the server (in the SYN,ACK).

  Workaround: Disable TCP Window Scaling on either the server or on the client.

- CSCsl16482

  HTTP authentication with the **ssl trust-point** command is not working after you reload the FWSM. The CA certificate imported is not used after the reload. The following syslog message displays:

  ```
  %FWSM-3-717023: SSL failed to set device certificate for trustpoint <trustpoint>.
  Reason: No device certificate found.
  ```

  Workaround: Perform the following steps:

  a. Enter the **no crypto ca trustpoint** *trustpoint* command.
  b. Reimport the CA certificate.
  c. Enter the **ssl trust-point** *trustpoint* command.

- CSCsl29965

  The failover interfaces are not reported through SNMP. Snmpwalk shows all interfaces, except the failover ones.

  Workaround: None.

- CSCsl33529

  Packets might be passed by the standby FWSM in a failover pair during the short period of time that the FWSM is syncing just after booting.

  Workaround: None.

- CSCsl47376

  NAT exemption is not used for communication between same-security-level interfaces when you have other NAT types configured that match the traffic; NAT exemption is supposed to take priority over other NAT types.

  Workaround: Define a policy NAT statement to exclude hosts you wish to exempt.

- CSCsl67421

  If you enable SNMP traps when upgrading from 2.3(4) to 3.1(8), then the FWSM might experience a software-forced reload.

  Workaround: None.

- CSCsl68230

  URL-filtering-denied traffic is unsuccessfully closed; you can see the dropped traffic using the **show asp drop** command.

  Workaround: Disable the TCP normalizer by entering the **no control-point tcp-normalizer** command.

The caveats in Table 12 were resolved in Release 3.1(9), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 12 Caveats Resolved in Release 3.1(9)

Caveat ID	Title
CSCsd09483	SRFW: Disabling PIM on one interface cause the whole IGMP not working
CSCsj81538	FWSM running 3.2(1) has ASR feature broken with transparent mode
CSCsk81211	DHCPrelay binding limit of 100 to be configurable for scalability
CSCsl11774	'sysopt connection timewait' has no effect on FWSM and should be removed
CSCsl24414	FWSM:BPDU keep passing through when intf shutdown in transparent context
CSCsl34625	FWSM crash in assert with c_bridge_group:bridge_group_action
CSCsl50309	FWSM crashes due to sunrpc inspection.
CSCsl52399	FTP inspection inserting incorrect PAT address
CSCsl57262	DHCP discover is dropped by FWSM
CSCsl57838	Config replication under heavy fast-path load causes NP hang
CSCsl60126	Converting rpc and rpc_udp fixups to MPF triggers redundant sunrpc
CSCsl65187	FWSM: crash in telnet/ci capture:destroy_capture
CSCsl70414	'write standby' on FWSM reintroduces default policy map on standby
CSCsl76792	Parser Cleanup - passwords should be adjacent to each other
CSCsl89773	Cos/DSCP of Failover packet is 0, not 5
CSCsl97424	FWSM displays inconsistent value for 'Configuration last modified'
CSCsm01604	Ping command with no destination ip specified causes crash
CSCsm11988	Unable to clear uauth entry by username if username includes backslash
CSCsm27076	SMTP Fixup dropping 64-byte DATA packet that has 4 zeroes of padding

Resolved Caveats in Software Release 3.1(8)

- 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 in this example are 1025 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.

   17664 is 0x4500 in hexadecimal.

b. Exchange the hexadecimal byte pairs. For example:

   0x0104 exchanged is 0x0401.

   0x4500 exchanged is 0x0045.

c. Convert the exchanged hexadecimal number to decimal to get the true port number. For example:

   0x0401 is 1025 in decimal.

   0x0045 is 69 in decimal.

- CSCsg49036

  The **show memory detail** command indicates 399% or 400% for the used memory in the admin context:

```
hostname# changeto context admin
hostname/admin#
hostname/admin# show mem detail
Used memory:      4294561916 bytes (400%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)

Most used memory: -    36676 bytes (400%)
```

  Workaround: None.

- CSCsh99789

  If you configure URL filtering for HTTPS, then HTTPS sessions are subject to URL filtering in both the outbound direction (high security to low security interface), which is expected, and the inbound direction (low security to high security interface), which is not expected. For HTTP and FTP, only outbound connections are filtered.

  Workaround: None.

- CSCsi05221

  When traffic hits an ACE while swapping the ACE order, the access list logging stops. For example, after swapping the ACEs of the below access list:

```
access-list vbug extended permit ip host 10.1.1.2 host 10.0.0.100 log interval 10
access-list vbug extended deny ip host 10.1.1.5 host 10.0.0.100 log interval 10
```

  To:

```
access-list vbug extended deny ip host 10.1.1.5 host 10.0.0.100 log interval 10
access-list vbug extended permit ip host 10.1.1.2 host 10.0.0.100 log interval 10
```

  Logs for the permit ACE stop showing up on the console.

  Workaround: Stop the traffic, remove the access list, reconfigure it, and reapply.

- CSCsi07224

  When traffic matches an ACE, a system log message is generated in the syslog even though logging has been disabled for this ACE. For example:

```
hostname(config)# access-list outside_in line 16 extended deny tcp host
192.168.120.103 host 172.16.1.28 eq https log disable

Mar 09 2007 18:35:07 VFW1 : %FWSM-1-106100: access-list outside_in denied tcp
outside/192.168.120.103(32365) -> DMZ2/172.16.1.28(443) hit-cnt 1 (first hit)
[0x1a9ac098, 0x24cf570]
```

Workaround: None.

- CSCsi18503

  Free memory on an FWSM slowly decreases over time until no free memory is available, leading to an outage. H323 RAS inspection must be enabled and non-H323 traffic on UDP/1718 and UDP/1719 must be present. This traffic will be dropped by the inspection because it is not H323 RAS traffic.

  Workaround: Disable H323 RAS inspection. If this breaks H323 functionality, continuously monitor memory consumption on the FWSM and reload the FWSM when a critical level is reached.

  You can verify the drops by looking at the output of the **show service-policy** command.

- CSCsi60064

  When the ICMP inspection is not enabled, if the FWSM could not route the packet from a low security source host to a high security destination host, it sends an ICMP network unreachable error back to the source host with the real IP address of the destination tried, instead of the mapped address. Also, a traceroute from a low security interface to a high security interface returns the real IP address of the destination to the source host.

  Workaround: Configure ICMP inspection by entering the following commands:

  ```
  policy-map global_policy
   class inspection_default
     inspect icmp
  ```

- CSCsk15655

  You cannot delete counters of all access lists by using the **clear access-list counters** command.

  Workaround: You can only delete counters of access lists individually using the **clear access-list** *id* **counters** command.

- CSCsk19447

  When using the **config net** command on the FWSM to copy a configuration from a TFTP server to the running configuration, requests with long file names (more than 56 characters) fail or produce unexpected results.

  For example:

  ```
  config net 192.168.1.100:configurations/filename
  ```

  where *filename* is longer than 56 characters.

  Workaround: Use shorter configuration filenames.

- CSCsk21233

  If you reload the FWSM and you are prompted to save the configuration, then choosing the Save All option only saves the system configuration and not the security context configurations.

  Workaround: Enter the **write memory all** command in the system execution space before you reload.

- CSCsk23179

If you have the maximum of 5 **hsi-group** commands in an **h225-map**, and you remove one or more groups, then you cannot add a new **hsi-group** command or edit an existing one.

Workaround: You must remove the whole **h225-map** and create a new one.

- CSCsk25334

  Changing an interface name causes a memory leak on active and standby FWSMs.

  Workaround: None.

- CSCsk31912

  In manual commit mode, inactive access lists remain active after they are committed.

  Workaround: Use auto-commit mode.

- CSCsk40614

  A lot of packets are exchanged between the FWSM and a host in a matter of milliseconds if out-of-order packets arrive on the FWSM in some situations. This situation occurs when the TCP sequence number of a flow changes on either side of the FWSM due to a change in the data payload when NAT is configured.

  Workaround: Do not configure NAT.

- CSCsk44745

  If you have a failover pair, and you have to replace or redeploy the standby unit, then when you start up the new unit, failover becomes enabled even if the failover VLAN is not yet assigned from the switch, or if the switch is slow in assigning the VLAN. Therefore, the failover link is not active between the two units.

  This situation can cause a number of problems; for example, the new unit becomes active, so you have two active units on the network. Then, when the VLAN is finally assigned to the new unit, if the new unit is designated as the primary, it forces the secondary unit to become standby. At best, this causes an unnecessary failover event, and at worst the primary unit becomes active before you have finished configuring it; the good configuration on the secondary unit gets overwritten by the bad configuration on the primary.

  Workaround: Always assign the failover VLAN to both units before you enable failover. Also, be sure to have a complete configuration on the primary unit before you deploy it, even if it is the standby unit.

- CSCsk49642

  If you configure the half-closed timeout using the **set connection timeout half-closed** command in a policy map, then the half-closed connections do not get cleared.

  Workaround: Set the global timeout using the **timeout half-closed** command. This timeout affects all connections, and not just those specified in the class map.

- CSCsk50020

  Authentication fails for an HTTPS session if the destination configured in an access list for AAA is a name that you associated with the IP address using the **name** command.

  Workaround: Do not use the name in the access list; instead use the actual IP address.

The caveats in Table 13 were resolved in Release 3.1(8), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 13 Caveats Resolved in Release 3.1(8)

Caveat ID	Title
CSCse14356	Its not possible to clear single conn with clear conn on 3.1.1
CSCsi24332	FWSM - slow memory leak when filter ftp enabled
CSCsi62117	FWSM crash Thread Name: fast_fixup
CSCsi75239	CLI same-security-traffic permit intra-interface help is incorrect
CSCsj66878	Write Memory All' Does Not Return Error Status on Failed Flash Write
CSCsj78808	FWSM crash in threadname SSH
CSCsk00270	FWSM 3.2 - RTSP inspect only uses first address in PAT pool
CSCsk28899	snmp-server without community is causing zombie output in other contexts
CSCsk34299	Can't del ACL used by capture in manual-commit mode using clear config
CSCsk71402	fwsm - cannot add static mac-address-table entry
CSCsk72522	Unable to add access-list error rc=0xc014
CSCsk76920	FWSM TCP Proxy Fails when TCP Window Scaling is Used
CSCsk78770	'copy running-config tftp:' fails from user context in multiple mode
CSCsk83269	SunRPC fails through FWSM with PAT after upgrade to 3.1
CSCsk94695	FWSM : RTSP may not work in multi-context mode
CSCsk99071	FWSM sends grat. arp on bootup even when interface shutdown
CSCsl02516	FWSM : RTSP inspect unexpectedly translates the User-Agent Field
CSCsl04910	ACL change causes high CPU and possible network outage
CSCsl09499	FWSM - DNS rewrite not applicable for Static PAT
CSCsl12104	Modifing fixup protocol icmp at a context affects other contexts (3.1)
CSCsl12381	Restore ability to copy captures off FWSM in Single mode via HTTPS
CSCsl29505	FWSM does not free up RADIUS IDs when there are many rejects
CSCsl49354	BPDU pass after shutting outside interface inside data context in TFW

Resolved Caveats in Software Release 3.1(7)

- CSCsg93070

  Currently, captures from the FWSM can only be retrieved from the FWSM using HTTPS in single context mode. In multiple context mode, another method must be used to transfer the captures of the FWSM.

  Workaround: Use TFTP to transfer the captures from the FWSM in the system execution space.

Note The FWSM uses the IP address of the admin context to transfer the files, but the command is only valid in the system execution space.

- CSCsi00694

  Malformed MGCP packets cause an unexpected reload of the FWSM when the MGCP inspection engine is enabled.

  Workaround: None.

- CSCsi15190

  The FWSM can experience a problem processing the FTP PORT command for active FTP sessions (when FTP inspection is enabled). This can prevent FTP data streams from flowing properly through the FWSM and prevent file transfer.

  Workaround: Disable the TCP normalizer using the **no control-point tcp-normalizer** command (introduced in version 3.1.4(9))

  This command has side effects: some voice-related inspections do not work properly after you disable TCP normalization, including H.323 and Skinny.

- CSCsi73723

  The FWSM sends system log message 106101 (“The number of ACL log deny-flows has reached limit *number*”) when the total amount of deny flows is far beneath the configured limit.

  Workaround: Disable the **log** option in the **access-list** entries.

- CSCsi86017

  After running a script that issues **show** commands, there was a memory loss of approximately 155 KB. When running the same script for just **show running-config** commands, there was a loss of approximately 100 KB of memory that was not recovered.

  Workaround: None.

- CSCsi90923

  A capture shows extra packets while capturing fragments. When the FWSM receives fragments, the accelerated path sends them to the session management path. The session management path collects these fragments, and after the final fragment is received, it reassembles them and sends the complete packet back again to the accelerated path for processing. Currently we capture this packet as well.

  Workaround: None.

- CSCsj18692

  The number of xlate entries shown in the standby unit is greater than the system limitation, which is 256 K entries. This problem is seen in standby unit when FWSM is configured to process outside PAT.

  Workaround: None.

- CSCsj25708

  In manual mode, access list logging does not work if you replace an ACE without logging enabled with an ACE that has logging enabled.

  Workaround: Use auto mode, or remove the existing ACE and then reapply the ACE with logging.

- CSCsj26805

  A client can successfully Telnet to the virtual *HTTP* IP address and get authenticated. Similarly, a client can successfully HTTP to the virtual *Telnet* IP address and get authenticated.

Workaround: None.

- CSCsj30459

  The **warning** keyword is not configurable with the **virtual http** command.

  Workaround: None.

The caveats in Table 14 were resolved in Release 3.1(7), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 14 Caveats Resolved in Release 3.1(7)

Caveat ID	Title
CSCeh42997	Perfmon interval stats output goes to the console instead of session
CSCsc33385	GTP - pdp context creation failed - GSN tunnel limit exceeded
CSCsd16751	GTP: wrong service-policy used when connection is re-used
CSCsg89646	The default timeout for the H.245 has been changed to 5 mins
CSCsg92895	copy ftp from firewall fails when default passive mode is used
CSCsg93070	Need ability to copy capture off via HTTPS in multi-context mode
CSCsh90098	Failover doesn't get re-activated after reload due to wrong VLAN mapping
CSCsi15190	FTP PORT command not processed when TCP Normalizer is active
CSCsi42756	FWSM memory leak when adding and removing context
CSCsi48952	Multicast traffic builds invalid xlate causing traffic interruption
CSCsi63925	Auth proxy generates login form with server IP address instead of name
CSCsi73723	106101 syslog is sent while total amount of deny flows is lower than max
CSCsi94230	SSH,Ping FWSM outside interface failure after failover
CSCsi96676	Local authentication password fails following upgrade
CSCsj09074	FWSM: norandomseq does not work with NAT exemption
CSCsj22526	FWSM running 2.3.4.10 or later may stop creating new connections.
CSCsj25708	ACL logging does not log when ACE has logging enabled
CSCsj29497	Primary FWSM Becoms Active When VLANs are Assigned
CSCsj31627	Perfmon Counters Don't Display Automatically on Telnet/SSH Sessions
CSCsj32385	Crash in dhcp_relay_agent_receiver
CSCsj38762	Applying crypto map without isakmp to an interface causes crash
CSCsj41942	Crash in fast_fixup while executing no control-point tcp-normalizer
CSCsj42148	Syslog 405001 reports incorrect IP when arp collision detected
CSCsj43708	UDP timeout of 4 minutes on FWSM may prevent connections from timing out
CSCsj43941	CSM deploys in speed mode of changes to object-groups cause issues
CSCsj46090	Failover : Primary doesn't get back to Active on rare situation
CSCsj51207	FWSM 3.1.6 Reload after show blocks all packet command
CSCsj52536	traffic does not hit ACLs after modified the ACLs

Table 14 Caveats Resolved in Release 3.1(7) (continued)

Caveat ID	Title
CSCsj53485	ICMP Traceroute Fails Across an FWSM
CSCsj56721	Setting TCP timers in MPF causes zombie UDP and half-closed TCP conns
CSCsj57188	FWSM calculates wrong checksum on re- transmitted packets
CSCsj57466	packets captured counter increments when capture buffer full
CSCsj65119	DHCP initial packet not passing via FWSM 3.1(6) transparent mode
CSCsj69977	Ethertype ACL got corrupted after reload
CSCsj72115	transparent FWSM : cross BVI xlates created by skinny inspection
CSCsj79986	multicast not streaming from source if igmp client on same vlan
CSCsj82706	FWSM syn cookie sending syn packet to server with mss=0
CSCsj95047	FWSM crash in telnet/ci thread when trying to add access-list
CSCsk03792	auth-proxy service getting stuck on FWSM
CSCsk06389	Drop IPv6 packets with non-zero flow label value
CSCsk08843	Debug and Access Rules Download Complete Messages Not Displayed on SSH
CSCsk11608	Add a cli to schedule the group queue
CSCsk17801	SNMP V2 Traps from FWSM
CSCsk26743	ASA Radius state machine reuses state attribute from failed auth
CSCsk32932	In multiple context mode, interfaces with mapped_names not usable/config

Resolved Caveats in Software Release 3.1(6)

- 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.

- CSCse95480

  Under a high load of SunRPC traffic, the standby unit might experience a crash after failover or after configuration replication.

  Workaround: None.

- CSCsh99987

  Capture does not work properly with fragmented packets.

  Workaround: None.

- CSCsi41905

  The packet capture tool does not capture all packets from the TCP session initialization sequence. When capture is configured to capture all TCP packets, for example, using a **permit tcp any any** access list, the capture buffer shows only the first SYN and the last ACK packets of the TCP session initialization. The buffer does not have the SYN_ACK packet.

  Workaround: None.

- CSCsh71532

  An access list of approximately 74 K ACEs with 151 K nodes takes more then 90 minutes to install and compile on the FWSM without any traffic.

  Workaround: None.

- CSCsg97419

  The FWSM resets with a show crash traceback of thread name doorbell poll.

  Workaround: None.

- CSCsi10027

  When IPv6 capture is defined for an interface, all IPv6 packets on that particular interface are captured, irrespective of the access list attached to the capture.

  Workaround: None.

- CSCsi32341

  You cannot reduce the circular buffer size for the **capture** command, once configured.

  Workaround: Remove the **capture** command, and reconfigure the capture again.

- CSCsi13442

  The OSPF neighbor goes down after changing the interface IPv6 setting. The FWSM sends OSPF hellos, but debugging does not show receiving OSPF hellos.

  Workaround: None.

- CSCsi26466

  A failure when compiling rules can cause some previously compiled rules to be removed under some special conditions. The previously compiled rules might get deleted from the configuration when there is any subsequent failed compilation of rules after more than 255 times of previous access list rule compilation.

  The current Compilation ID and number of time of rule compilation can be seen by entering the **debug acl download** command before updating the rules.

  Workaround: Reapply the previously-configured rules, including the startup configuration rules.

- CSCsi35494

  When the FWSM receives more numbers of packets than what it can hold in the capture buffer, the FWSM stops capturing packets for the linear buffer, but for the circular buffer, the capture continues by flushing out the earlier captured packets. So for the circular buffer, the total capture count will keep incrementing, but the number of packets shown will be limited by the buffer size.

  Workaround: None.

- CSCsi40318

  The FWSM does not print the following system log message when the wrong credentials are entered during AAA authentication for virtual SSH with ACS (RADIUS or TACACS+):

  ```
  %FWSM-6-611102: User authentication failed: Uname: user
  ```

  Workaround: None.

- CSCsi40607

  When a client attempts a traceroute through the FWSM, the ICMP error inspection engine does not allow the TTL expired messages to return to the client.

  Workaround: None.

- CSCsi48952

  Under rare circumstances, multicast packets processed by the FWSM might cause the FWSM to build incorrect translations in its translation table. This situation then results in the FWSM dropping TCP and UDP traffic sourced from the host that sent the multicast traffic.

  All of the following conditions must be met:

  - Multicast routing must be enabled on the FWSM.
  - NAT control must be disabled on the FWSM.
  - The xlate that is built is considered an inside xlate (**show xlate detail** shows the flag 'i')

  Workaround: To clear the incorrect translation, enter the **clear xlate local** *x* command where *x* is the IP address of the host that sent the multicast traffic and can no longer communicate through the FWSM.

  See the following example.

  Sample incorrect translation (**show xlate debug**):

  ```
  NAT from outside:192.168.1.100 to inside:192.168.1.100 flags si idle 0:00:55 timeout
  0:01:00 connections 1
  ```

  This translation shows that the host 192.168.1.100 is off of the outside interface of the FWSM, but the flags for the xlate show "si" indicating that the FWSM considers this an inside xlate, which is incorrect (this should be an outside xlate).

  To clear the translation, enter:

  ```
  hostname# clear xlate local 192.168.1.100
  ```

  Then, to prevent the incorrect translation from forming again do one of the following:

  - Disable multicast routing on the FWSM (or disable IGMP and PIM on a per-interface basis).
  - Apply an inbound access list on the interface where the host resides that blocks all traffic destined to the particular multicast address.

- CSCsi53621

  Capture of packets fails for a VLAN when a context that shares that VLAN is removed.

  For example, R1 and R3 contexts have a shared VLAN 200.

  Ping from outside host A to inside host B.

  When capture is enabled only in R1, inside1 and outside1 interfaces, both interfaces are able to capture packets.

  Now, enable capture in R3 in the shared VLAN. For a shared VLAN (VLAN 200 shared between R1 and R3), if you define a capture on both contexts, packet capture will happen only in the context where the capture was configured last. As expected, you should be able to see packet capture in inside3 and not inside1.

  If you remove R3, and go back to R1 and configure capture again, R1 inside1 should be able to capture packets now that the VLAN is not shared, but capture fails.

  Workaround: Disable and reenable capture.

The caveats in Table 15 were resolved in Release 3.1(6), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 15 Caveats Resolved in Release 3.1(6)

Caveat ID	Title
CSCef27422	OSPF does not install better route upon cost change
CSCse52237	not sending null register to RP when src and receiver directly attached
CSCse91999	Traceback in Thread Name: IKE Daemon with malformed ISAKMP packet
CSCse95480	crash in xlate.c during nfs traffic using PAT configuration
CSCsg80240	FWSM may report being out of translation slots
CSCsh81111	Denial-of-Service in VPNs with password expiry
CSCsi07168	primary shows that the secondary is standby ready when standby is shut
CSCsi13442	FWSM enabling ipv6 on interfaces causes ospfv2 adjacency down
CSCsi24838	Running Activation Key is not valid
CSCsi26466	All rules get deleted after reaching max nodes
CSCsi28206	FWSM multictx transp. failover - xlates on standby affects failover
CSCsi28206	FWSM multictx transp. failover - xlates on standby affects failover
CSCsi35772	SMTP fixup consistently drops '250 Ok' SMTP reply
CSCsi50428	FWSM clearing the DSCP values when skinny inspection is enabled.
CSCsi50544	Sup720:FWSM:mul context:ping/arp fails on shared outside vlan 4094
CSCsi53165	FWSM running 3.1.4 has ASR feature broken with transparent mode
CSCsi58010	FWSM:LU allocate xlate failed on standby unit
CSCsi60894	IPSG allowing L3 pkts with Valid MAC and Invalid IP when port comes up
CSCsi63011	FWSM service-policy command causes high cpu (also possible failover)
CSCsi63155	the CPU usage of one of the context goes up to 60% and it stays there
CSCsi75805	FWSM transparent mode allows telnet to outside interface
CSCsi75817	outgoing packet greater than 9k hangs the NIC
CSCsi77477	FWSM - Syslog 302020 doesn't include {in|out}bound direction information
CSCsi79428	FWSM 3.1.4 may reload when viewing running configuration.
CSCsi83484	LU allocate xlate failed message seen during traffic load test
CSCsi87893	Strange output may appear while configuing tftp-server parameters
CSCsi90898	'pim rp-address ' not replicated to the standby
CSCsi90927	SIP inspection should not try to NAT and reject VIA 127.0.0.1 headers
CSCsi92378	Fover: Primary Standby sends GARP with Active MAC when start-up
CSCsi95040	Connection-limits discrepancy between Syslog Message and show output
CSCsj02835	FWSM standby show Primary Active as Secondary Active during config sync
CSCsj04323	non ftp/telnet/htttp traffic triggers authentication process

Table 15 Caveats Resolved in Release 3.1(6) (continued)

Caveat ID	Title
CSCsj07948	management-access inside causes crash when FWSM brings up L2L Tunnel
CSCsj12108	FWSM not allocating the PAT xlate for secondary channel for FTP.
CSCsj17171	FWSM: Failed adding/deleting Rule to classifier
CSCsj19133	ICMP type 3 code 4 : icmp inspection does not translate port in payload

Resolved Caveats in Software Release 3.1(5)

- CSCsh19435

  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.

- 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.

- CSCse90329

  No error message is generated when an access list associated with the **aaa authentication match** command is removed; all **aaa authentication match** commands are removed when you delete the associated access list.

  Workaround: None.

The caveats in Table 16 were resolved in Release 3.1(5), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

http://www.cisco.com/support/bugtools

Table 16 Caveats Resolved in Release 3.1(5)

Caveat ID	Title
CSCsd23802	FWSM has very high CPU utilization with a large ACL configuration
CSCse52237	not sending null register to RP when src and receiver directly attached
CSCsf16544	FWSM - ssh thread never ends up when aaa authentication fails
CSCsf30620	transparent FWSM : cross bridge-group/BVI xlates within the same context
CSCsg00377	show resource usage command reports incorrect connection usage
CSCsg21497	FWSM 3.x ftpclient uses relative path while 2.x uses absolute path [DOC]

Table 16 Caveats Resolved in Release 3.1(5) (continued)

Caveat ID	Title
CSCsg27325	SSL Cut-through proxy is incompatible with MAC Safari browser
CSCsg47016	Change syntax of syslog 109003 to indicate immediate reactivation
CSCsg49938	FWSM crashes at Thread PIM IPv4
CSCsg51266	Multicast through FWSM may result in mismatch between NP and PC tables
CSCsg53682	FWSM failover - Configuration Replication takes a very long time
CSCsg59175	FWSM 3.1.3 URL-Filtering http Redirect failure
CSCsg70876	FWSM sends TCP reset packet when primary unit boots up
CSCsg81657	pptp inspection not working if both PAT and static policy NAT configured
CSCsg85361	FWSM 3.1.3 UnProxy Failed when extra keystrokes sent to Uauth session.
CSCsg92416	capture <name> type asp-drop feature missing
CSCsg94063	FWSM 3.1.3.23 does not forward SYN ACK with Zero Window w/ http inspect
CSCsg94695	FWSM invalid error message when adding new static when static policy pat
CSCsg96196	MPF set timeout tcp 0 not applied and overridden by global timeout
CSCsg98057	NP - CP communication limits 16384 blocks to 5500
CSCsg98660	Syslog 305012 - Teardown dynamic translation is not generated
CSCsh04159	FWSM slow memory leak in url-cache process for URL filtering
CSCsh06935	DOC: Transparent mode when multiple subnets transported on L2
CSCsh07125	FWSM - static PAT statements break nat 0 ACL
CSCsh11110	Cant Ping Admin context after adding or removing a context
CSCsh18755	access-list log disable still logs messages when access-list is hit
CSCsh18916	FWSM: identity translation can be created for an interface on FWSM
CSCsh19435	FWSM Ping/All traffic drops w/ join-failover-group and failover disabled
CSCsh20088	Crash while ping on failover link with packet size 8782
CSCsh20582	DOC - control-point tcp-normalizer command needs to be documented
CSCsh22071	FWSM 3.1.4 show np 3 aaa stats counter AAA Lookup Failures Incrementing
CSCsh24762	Release notes inconsistent with bug toolkit CSCsd35168
CSCsh30070	FWSM TFTP inspect- connection created on port 0, drops error packets
CSCsh30951	Crash in thread name Door Bell Poll
CSCsh32023	FWSM accepts wildcard mask for ip local pool
CSCsh32804	Syslog message 411003 not correctly documented
CSCsh41522	Logging queue 0 is wrongly shown as being unlimited queue
CSCsh42746	Documentation correction - FWSM does not support aaa accounting http
CSCsh48047	FWSM 3.1 messages documentation does not document %FWSM-6-605005
CSCsh49717	Need to add IP land attack checks to ingress packet processing
CSCsh51650	acl hitcnt for policy nat is doubled
CSCsh53177	upgrading from 3.1.3 to 3.1.4 sometimes crashes the standby fwsm

Table 16 Caveats Resolved in Release 3.1(5) (continued)

Caveat ID	Title
CSCsh53295	NAT Translations not working correctly
CSCsh59609	FWSM 3.1.4 failover group setup results in MAC address to be all 0's
CSCsh61313	ACEs and system access rules are removed from config without error msg
CSCsh63256	FWSM sets a CFI bit in dot1q header for traffic routed by FWSM
CSCsh64092	Active/Active : 'Failover Stop Traffic' flags unexpectedly set to 1
CSCsh67596	TFW: Arp flowing across the box is not updating the bridge-timeout
CSCsh68423	FWSM crash in fast_fixup due to SUNRPC inspection
CSCsh70631	FWSM Capture multi-context shared interface ingress or egress packets
CSCsh75142	Cannot rename interface after remove/add its VLAN to context
CSCsh84334	ssh process never terminates if aaa server does not respond
CSCsh90052	Error message missing, if failover activation is failing
CSCsh92908	FWSM in failover deletes static routes from configuration
CSCsh97689	Upgrade from 2.x - 3.x allocate-interface map_ifc string is lost
CSCsi01482	FWSM 3.1.3 http redirect command not available
CSCsi05248	ICMP unreachable messages fail through FWSM with inspect icmp error
CSCsi12105	mac-addresses found on failover vlans generate static table entries
CSCsi27367	Traceback in Thread Name: arp_forward_thread

Resolved Caveats in Software Release 3.1(4)

- 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.

- 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.

- 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 system log message 305006.

  Workaround: None.

- 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 Release 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.

- 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

  Modifications to an access list sometimes leads to a misordering of ACEs in the access list, which leads to incorrect access list filtering. This situation only occurs if an ACE includes an object group.

  Workaround: None.

- 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.

- 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.

- 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

  When you perform an 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.

- CSCse95822

  If you change the logging level of system log message 106100 from 6 to a lower level using the **access-list** command **log** *level* argument, the FWSM does not recognize the new level; you can only view the message if you show messages for level 6 or 7 (informational or debugging).

  Workaround: View level 6 or 7 logging messages.

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 5 K, change the MTU size on the outgoing interface of the FWSM to a larger value, like 8 K. 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 43
- Software Documents, page 43

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 and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.