



# Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 2.3(x)

---

**July 2006**

This document contains release information for the following FWSM Releases:

- 2.3(5)
- 2.3(4)
- 2.3(3)
- 2.3(2)
- 2.3(1)



**Note**

The FWSM 2.3(3.2) and later releases passed Cisco Safe Harbor testing in single routed firewall mode and in single transparent firewall mode.

---

This document includes the following sections:

- [Important Notes, page 2](#)
- [Chassis System Requirements, page 2](#)
- [Management Support, page 3](#)
- [New Features, page 4](#)
- [Upgrading the Software, page 5](#)
- [Software License Information, page 5](#)
- [Limitations and Restrictions, page 5](#)
- [Open Caveats in Software Release 2.3, page 7](#)
- [Resolved Caveats in Software Release 2.3\(5\), page 12](#)
- [Resolved Caveats in Software Release 2.3\(4\), page 14](#)
- [Resolved Caveats in Software Release 2.3\(3.2\), page 17](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Resolved Caveats in Software Release 2.3\(3\), page 18](#)
- [Resolved Caveats in Software Release 2.3\(2\), page 25](#)
- [Resolved Caveats in Software Release 2.3\(1\), page 27](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 31](#)

## Important Notes

See the following important notes for configuring the FWSM:

- In some circumstances, when you configure a limit on TCP connections as well as a limit on embryonic connections in a **nat** or **static** statement, a denial of service (DoS) condition might occur. We recommend that you configure only one of these limits at a time for a given **nat** or **static** statement, and leave the other at the default of 0 (unlimited, up to the maximum for the system). The UDP connection limits are not affected. See caveat CSCee47998 for more information.
- When you configure the embryonic limit for an inside **static** statement, and you also configure dynamic PAT for an outside interface, then a SYN attack from the outside to the inside static address causes a large number of PAT translations with associated connections, even though the connections are not established. These PAT translations do not time out within the default 30-second interval for translations without the associated connections because the FWSM thinks that there are valid connections associated. The pool of addresses and ports for the outside addresses gets used up, and no additional clients can connect. We recommend that you do not configure outside PAT in this situation. See caveat CSCee48769 for more information.

## 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 *or* Catalyst operating system (OS). See [Table 1](#) for supported supervisor engine and software releases.
  - Multilayer Switch Feature Card (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.

[Table 1](#) shows the supervisor engine version, software, and supported FWSM features.

**Table 1 Support for FWSM 2.3 Features**

	Supervisor Engines <sup>1</sup>	FWSM Features:	
		Multiple SVIs <sup>2</sup>	Transparent Firewall with Failover <sup>3</sup>
<b>Cisco IOS</b>			
12.1(13)E	2	No	No
12.1(19)E	2	Yes	No
12.1(22)E and higher	2	Yes	Yes
12.2(14)SY and higher	2	Yes	No
12.2(14)SX	2, 720	No	No
12.2(17a)SX3	2, 720	Yes	Yes
12.2(17b)SXA	2, 720	Yes	Yes
12.2(17d)SXB and higher	2, 720	Yes	Yes
12.2(18)SXF	32, 2, 720	Yes	Yes
<b>Catalyst OS<sup>4</sup></b>			
7.5(x)	2	No	No
7.6(1) through 7.6(4)	2	Yes	No
7.6(5) and higher	2	Yes	Yes
8.2(x)	2, 720	Yes	Yes
8.3(x)	2, 720	Yes	Yes

1. The FWSM does not support Supervisor Engine 1 or 1A.
2. Supports multiple switched VLAN interfaces (SVIs) between the MSFC and FWSM. An SVI is a VLAN interface that is routed on the MSFC.
3. Supports transparent firewall mode when you use failover. Failover requires BPDU forwarding to the FWSM, or else you can have a loop. Other releases that do not support BPDU forwarding only support transparent mode without failover.
4. When you use Catalyst OS on the supervisor engine, you can use any of the supported Cisco IOS releases above on the MSFC. (When you use Cisco IOS software on the supervisor engine, you use the same release on the MSFC.) The supervisor engine software determines the FWSM feature support. For example, if you use Catalyst software release 7.6(1) on the supervisor engine and Cisco IOS Release 12.1(13)E on the MSFC, then the switch does support multiple SVIs, because Catalyst software release 7.6(1) supports multiple SVIs.

## Management Support

The FWSM supports the following management methods:

- Cisco ASDM—Software Release 4.1 supports FWSM software release 2.3 features. PDM 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.
- Cisco Firewall MC—Software release 1.3.1 supports FWSM software release 2.3 features. For multiple context mode, software release 1.3.1 supports management of each context separately but does not support system-level operations, such as adding or deleting contexts, or the provisioning of failover in multiple mode.

- 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 2.3(1).

**Table 2**      **New Features**

Feature	Description
Enabling secure authentication of web clients	FWSM software release 2.3 introduces a secured method of exchanging usernames and passwords between a web client and an FWSM by using HTTP over SSL (HTTPS). HTTPS encrypts the username and password and makes the transmission secure. FWSM software release 2.3 also supports authentication of HTTPS connections.
Per-user access list override	In FWSM software release 2.3, the per-user access list overrides the interface access list, regardless of the status of the interface access list. In previous releases, the user traffic was subjected to both the interface access list and per-user access list checking.  See the <b>access group</b> command.
SYN cookies	The TCP intercept feature implements software to protect the TCP servers from the TCP SYN-flooding attacks, which are a type of denial-of-service attack. SYN cookies are used during the validation process and help to minimize the amount of valid traffic being dropped.
Per-host connection limit in same security level communication	The introduction of the Same Security Level Communication (SSLC) feature meant that it was no longer possible to define which interface is the inside (protected) host and which interface is the outside (unprotected) host. Both hosts belong to the interfaces at the same security level. This situation eliminates the need to restrict the maximum connection limit to a particular interface. Any host on any interface can initiate or receive a session to or from any host or server in any other interface. This feature accounts for all the possible connections to and from any host. This feature will be enabled by default for communication between the interfaces on the same security level when SSLC is enabled.
Autostate support	FWSM software release 2.3 applies the Catalyst 6500 series switch supervisor engine auto-state functionality to the FWSM in order to improve the accuracy and performance of the interface monitoring feature. Auto-state is used by the supervisor engine to send a message to the modules whenever physical ports leave or join a VLAN. Autostate is supported in Catalyst operating system software release 8.4(1) only.
Disabling automatic configuration synchronization	Management applications may lose connectivity when upgrading the FWSM with complex configurations. This can result in incomplete configuration files being applied to the standby FWSM. Starting with FWSM software release 2.3, you can disable the automatic configuration synchronization in order to avoid incomplete configurations being applied to the standby FWSM.

**Table 2**      **New Features (continued)**

Feature	Description
access list memory partitions	Access list memory partitions allow you to maximize the available access list memory in the network processor when creating security contexts. The default access list memory is divided into 12 partitions and an additional backup partition. By default, each security context is assigned to an access list partition chosen in a round-robin manner. Starting with FWSM Release 2.3, you can configure the number of partitions so that you maximize access list memory usage.
Intra-interface communication	Prior to FWSM software release 2.3, packets reaching the firewall that were directed to a host in the same interface as the sender were dropped. Starting with FWSM software release 2.3, you can configure the FWSM to enable communication between two hosts on the same interface.

## Upgrading the Software

The following command allows you to upgrade from FWSM software release 1.1 (or pre-release versions of 2.x) to FWSM software release 2.3. For other upgrade options for upgrading from Release 2.x, such as upgrading to a different application partition or from a different type of server, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

To upgrade the application software to the current application partition, enter the following command. For multiple context mode, you must be in the system execution space.

```
hostname# copy tftp://server[/path]/filename flash:
```

For example, enter the following command:

```
hostname# copy tftp://209.165.200.226/cisco/c6svc-fw-9.2-1-1.bin flash:
```

## Software License Information

FWSM software release 2.2 introduced a software license for multiple security context support. With the basic license, the FWSM supports two contexts plus the special admin context. You can buy a license for additional security context support, up to 100 contexts. See the Cisco.com website for more information about licensing options. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for more information about entering a license activation key.

## Limitations and Restrictions

This section lists the limitations and restrictions for the following operating systems:

- [Limitations and Restrictions on the FWSM, page 6](#)
- [Limitations and Restrictions in Cisco IOS Software, page 6](#)
- [Limitations and Restrictions in the Catalyst Operating System, page 6](#)

## Limitations and Restrictions on the FWSM

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 two interfaces per context.
- For transparent firewall mode, you must configure a management IP address.
- The outbound connections (from a higher security interface to a lower security interface) from an interface that is shared between the contexts can only be classified and directed through the correct context if you configure a static translation for the destination IP address. This limitation makes cascading contexts unsupported, because configuring the static translations for all the outside hosts is not feasible.
- The CPU-intensive commands, such as **copy running-config startup-config** (and the **write memory** command, which performs the same task), 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.

## Limitations and Restrictions in Cisco IOS Software

See the following limitations and restrictions in Cisco IOS software for interoperating with the FWSM. See also the “[Chassis System Requirements](#)” section on page 2 for the FWSM feature support in Cisco IOS software.

- Although the FWSM can handle jumbo Ethernet frames, the switch does not handle jumbo frames through the FWSM. See caveat CSCee03625 for more information.
- For some releases of Cisco IOS software, you cannot install the FWSM in slot 13. This problem occurs with all service modules. See caveat CSCed82263 for more information.
- For some releases of Cisco IOS software, if the supervisor engine fails over, the FWSM switching mode might change from crossbar mode to bus mode. This change causes FWSM traffic to be disrupted until the switching mode returns to crossbar mode (see the **show fabric switching-mode** command to view the FWSM switching mode). You can restore the crossbar mode by bringing the failed supervisor engine online again by inserting a new crossbar module or by reloading the FWSM. See caveat CSCee62630 for more information.

## Limitations and Restrictions in the Catalyst Operating System

See the following limitations and restrictions in the Catalyst operating system for interoperating with the FWSM. See also the “[Chassis System Requirements](#)” section on page 2 for FWSM feature support.

- Although the FWSM can handle jumbo Ethernet frames, the switch does not handle jumbo frames through the FWSM. See caveat CSCee03625 for more information.
- If you reload the switch or the FWSM, the switch might lose the configuration that assigns the VLANs to the FWSM. You need to reenter the **set vlan firewall-vlan** command after the reload. See caveat CSCed69941 for more information. This problem is resolved in release 8.3(1) and might be resolved in earlier versions.

- If you reload the switch, the switch might lose the configuration for the SVIs on the MSFC. You need to reenter the **interface vlan** command on the MSFC after the reload. See caveat CSCed69931 for more information. This problem was found in software release 7.6(5) and might exist in later releases.

## Open Caveats in Software Release 2.3

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 2.3(2), then you need to add the caveats in this section to the resolved caveats from 2.3(3) and later to determine the complete list of open caveats.

If you are a registered cisco.com user, view Bug Toolkit on Cisco.com at the following website:

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

To become a registered Cisco.com user, go to the following website:

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

- CSCdz11283

Because the FWSM does not allow Telnet to the lowest security interface, if you configure a context with only one interface, you cannot Telnet to it because it is inherently the lowest security interface.

**Workaround:** Configure a second interface at a lower security level, and then delete the interface; the FWSM now allows Telnet to the one remaining interface.

- CSCea93521

If you change any **crypto map** commands, the changes are made in the configuration, but the FWSM still uses the old settings.

**Workaround:** Reapply the crypto map to the interface by entering the **no crypto map interface** command to remove it, and then reapply the crypto map.

- CSCeb00636

When you set the **fragment** command to 1, the **show fragment** command displays the value as 0. The FWSM uses the correct value of 1 even though the display is incorrect.

**Workaround:** None.

- CSCec02764

When you use Reflection X as an XDMCP client, the connection gets reset after 2 hours.

**Workaround:** Enter the **timeout conn** command to set the TCP connection timeout to 4 hours on the FWSM instead of the default of 1 hour.

- CSCed75337

When a duplicate route with a lower metric cost through a different interface is configured the **show route** command displays the incorrect interface.

**Workaround:** Remove the initial route that is going to be replaced and then configure the new route.

- CSCed92496

When a Smurf attack occurs against the FWSM, the FWSM correctly drops the traffic, but does not generate a system message or SNMP trap about the Smurf attack.

**Workaround:** None.

- CSCee25850  
In manual commit mode for access lists, the **show access-list** command shows the standard (OSPF) access lists as not being committed. The display is incorrect, and the standard access lists behave as expected.  
**Workaround:** None.
- CSCee29967  
In multiple context mode, the system execution space cannot send system messages to an external syslog server through the admin context; you can only view these system messages from the buffer or on your session monitor.  
**Workaround:** None.
- CSCee41620  
When you use Cisco VPN client Release 3.6.3 for management access in routed firewall mode, you cannot use the local database for user authentication.  
**Workaround:** Use RADIUS or TACACS+ for authentication.
- CSCee55112  
The CPU goes to 99 percent of capacity when there is a large number of SCCP sessions suddenly being handled. This situation negatively impacts IP routing updates.  
**Workaround:** None.
- CSCee78616  
Performance monitoring values do not match the statistics that the resource manager collects.  
**Workaround:** Use the **show resource usage** command to obtain accurate statistics.
- CSCef47137  
The duration value in the translation teardown syslog messages does not correspond to the real duration of the connection.  
**Workaround:** None.
- CSCef60476  
The problem occurs when an FWSM has several interfaces with the same security level and IP phones in a different VLAN than the Cisco CallManager and the phones register but when they go off hook, they do not get a dial tone and they reset.  
**Workaround:** Move the IP phones to the same VLAN that Cisco CallManager is on.
- CSCef77370  
When you enter the **show processes** command, the run-time values in the output are not accurate. During high CPU usage on the FWSM, the run-time values are used to determine which processes are using the CPU. Currently, the values are incremented only if the time that the process spends on the CPU is 1 millisecond (ms) or longer. Therefore, an active process that runs frequently on the CPU, but spends less than 1 ms each time, would show a run-time of 0.  
**Workaround:** None.
- CSCeg27568  
During heavy traffic load, the number of hit counts that are shown from the **show ethertype acl** output is incorrect.  
**Workaround:** None.
- CSCeh08578

The problem occurs with the following topology: an FWSM configured in routed mode with two networks, one inside and one outside, one Skinny phone a Cisco CallManager on the inside network, and an H323 gateway on the outside network.

When a call is placed between two skinny phones through the H323 gateway and one Skinny phone places the call on hold, the Cisco CallManager sends a music-on-hold (MOH) signal. This MOH signal is denied by the FWSM.

**Workaround:** Explicitly allow all UDP traffic from the Cisco Call Manager to the H.323 gateway.

- CSCeh46215

An OSPF route and a static route are configured with a higher administrative distance for the same prefix. Upon deletion of the OSPF route, the statically configured route for the same subnet does not operate.

**Workaround:** If possible, configure the supernet of the OSPF route as a static route so that the normal routing rules can operate correctly.

- CSCeh52794

The transparent firewall cannot learn the MAC addresses for forwarding packets when failover is enabled and mis-configured without having the failover VLAN mapped to the FWSM.

**Workaround:** Verify that the failover VLAN is mapped to FWSM when configuring failover settings.

- CSCeh94780

If two telnet sessions are directed to the same FWSM and both sessions cause the display to present the "more" prompt, one session will remain frozen until the other session enters a character.

**Workaround:** Use the **no pager** command so the display does not stop at the "More" prompt.

- CSCeh96321

When you enable URL caching, all HTTP traffic stops. The server is up, and as soon as caching is disabled normal traffic flow resumes.

**Workaround:** Disable URL caching.

- CSCsb88556

FWSM crashed at doorbell\_poll due to an assert in the slow path (NP3).

**Workaround:** None.

- CSCsb98776

OSPF convergence is not happening properly when OSPF authentication is configured between neighbors. When you first configure OSPF authentication on the FWSM and its neighbors, the convergence happens properly. If you then make the authentication fail by making the key mismatched, then changing the key to match again, then the convergence does not happen properly.

**Workaround:** None.

- CSCsd09987

System log message 313004 shows the following; the interface name is not shown for the source IP address.

```
Jan 6 07:16:08 172.16.197.100 %FWSM-4-313004: Denied ICMP type=11, from laddr
192.168.248.57 on interface to 10.109.230.127: no matching session
```

**Workaround:** None.

- CSCsd10442

A PDM Configuration Refresh hangs when another session is stopped at the <--- More ---> prompt. The PDM displays a window "Please wait while the PDM is loading the current configuration from your firewall." It has a progress bar and the bar hangs at 27%. Only if the first session finishes their display and gets past the <--- More ---> prompt will the progress bar finish out to 100%.

**Workaround:** Clear the <--- More ---> prompt from the user session.

- CSCsd13603

Conditional OSPF Default Route Advertisement does not work (the **default-information originate route-map** command); the FWSM does not conditionally advertise a default route based on the presence of another route on an FWSM.

**Workaround:** Configure a static recursive default route for a route learned via OSPF.

- CSCsd19916

In multiple context mode, when contexts include large access lists and established statements, then the compilation of access lists might fail, even if the maximum number of access lists is not reached for the memory partition the context is assigned to.

**Workaround:** Decrease the number of memory partitions to increase their size. See the following document for how to perform this change:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/fwsm/fwsm\\_2\\_3/fwsm\\_cfg/context.htm#wp1105979](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/fwsm/fwsm_2_3/fwsm_cfg/context.htm#wp1105979)

- CSCsd66880

The FWSM crashed with Thread Name: fast\_fixup. The crash occurred when the FWSM was inspecting FTP traffic.

**Workaround:** Disable the FTP inspection by entering the **no fixup ftp** command.

- CSCsd67726

The **write net** command fails in a context, even though the context can ping the TFTP server.

**Workaround:** None.

- CSCsd71029

When using manual commit to access list changes, changes made to access lists related to authentication match statements are not effective after the commitment.

**Workaround:** Use auto commit (the default). The workaround once the access list has become ineffective is to remove and re-insert the authentication match statement.

- CSCsd73727

When the FWSM CPU usage is high (due to a large access list compilation or other reasons), the SSL connection between the FWSM and CSM fails. The corresponding defect in CSM is CSCsd35974.

**Workaround:** None.

- CSCsd79002

In the **show np 3 acl count** output, the NP 3 ACL Uncommitted Add display increments when you add and remove the same access list in manual commit mode.

**Workaround:** None.

- CSCsd81986

AAA is configured for HTTP inbound traffic. FTP or ICMP traffic goes through fine without asking for authentication. But if the host is already authenticated through HTTP, FTP or ICMP traffic is denied. Per-user-override is not configured and dynamic access list permits HTTP. The interface access list permits all traffic.

**Workaround:** None.

- CSCsd85181

Under rare circumstances in multiple context routed mode with shared interfaces, some traffic flows might fail through the FWSM while others flow fine.

**Workaround:** Fail over to the standby FWSM if possible, and reload the failed FWSM.

- CSCsd85407

After removing a **name** command that is applied to **router ospf**, The area ID still shows the name. After entering **write standby** on the active FWSM, the standby FWSM keeps rebooting.

**Workaround:** None.

- CSCse77534

The DNS fixup translates a DNS response without the **dns** keyword configured in the **static** command.

For example, a reflector is configured with the following A Record:

```
www.cisco.com =192.168.2.104
```

The FWSM with the DNS fixup enabled has the following **static** command:

```
static (DMZ2,outside) 192.168.1.104 192.168.2.104 netmask 255.255.255.254
```

A client makes a DNS request to 192.168.1.104 for www.cisco.com and receives an answer of 192.168.1.104 when the answer should be 192.168.2.104.

**Workaround:** If **fixup protocol dns** is disabled, the correct response is received by the client.

- CSCsh11010

Zero downtime upgrades fail to work on the FWSM, resulting in both units in an Active state. For example, if one unit is upgraded to another 2.x release, during the version check process the existing Active unit will go into a Disabled state, but continue to pass traffic. The Standby unit will detect that the peer is not Active, and will become Active. At this point, both units are now attempting to pass traffic with the Active IPs.

**Workaround:** Install the new software on both units, and reboot them both at the same time, resulting in minimal down time.

- CSCsi44694

The FWSM unexpectedly stops passing traffic and reloads. This typically occurs at the moment a change is made to an object group.

**Workaround:** None.

- CSCsj52383

When a previous configuration on the FWSM is erased and the FWSM is rebooted, after the FWSM starts up, **access-list deny** flows are not created.

The following system log message is displayed on the console:

```
%FWSM-1-106101: Number of cached deny-flows for ACL log has reached limit (0)
```

**Workaround:** Reenter the **access-list deny-flow-max** command or save the current configuration and reboot the FWSM.

- CSCsj10277

If you connect to the switch console and session to the FWSM, if you enter the **show running-config** command and hold the space bar pressed, then the FWSM stops responding to keepalives from the switch; the switch then power cycles the FWSM.

**Workaround:** Do not hold the spacebar pressed down.

## Resolved Caveats in Software Release 2.3(5)

This section describes caveats closed in FWSM Release 2.3(5).

- CSCee54611

The FWSM does not reboot after you force a watchdog crash. After the forced crash, a message displays stating that the module will restart but it will not restart.

**Workaround:** None.

- CSCeh84289

FWSM may crash in response to a `doorbell_poll`, which causes the supervisor to reset each FWSM when there is traffic passing through the switch.

**Workaround:** None.

- CSCsd18537

In single routed mode with **fixup dns** configured, an FWSM might silently drop a DNS self-query when the client and DNS server are on separate VLANs. No system log message is produced by the FWSM.

**Workaround:** Remove DNS inspection by entering the **no fixup dns** command.

- CSCsd50667

In some instances, an access list blocks traffic that is supposed to be explicitly allowed.

**Workaround:** Reload the FWSM.

- CSCsd57518

An inbound TCP connection was established through the FWSM. At some point something happens to the network path, and packets are unable to get through. The endpoints know that the connection is down, but the FWSM does not. When the network is restored, the endpoints try to create a new connection but the FWSM thinks this connection is part of the previous one and tries to reset its connection timers. It should RST the previous flow and allow a new one.

**Workaround:** None.

- CSCsd67334

When an external authentication server is configured, and that server connectivity is somehow interrupted on the FWSM during SSH authentication attempts, then the SSH management connections to the FWSM are being refused or denied.

The **show resource usage** command indicates all SSH resources are being occupied:

Resource	Current	Peak	Limit	Denied	Context	
Telnet		1	2	5	0	System
SSH		5	5	5	501	System

A system log message is generated for the denied SSH session:

```
%FWSM-4-315005: SSH session limit exceeded. Connection request from X on interface
outside
```

**Workaround:** There is no workaround to clear out these SSH sessions without doing a reload of the FWSM. If you have a failover unit, you can fail over to the standby unit and reload the active unit having the issues. If this problem continually reoccurs, use local authentication until a fix is available.

The following caveats were fixed between Release 2.3(4) and 2.3(5), and were not previously documented.

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description.

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

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

To become a registered cisco.com user, go to the following website:

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

**Table 3** *Caveats Fixed between Release 2.3(4) and 2.3(5)*

Caveat ID	Title
CSCsi10418	Gratuitous ARP support in FWSM classifier
CSCsh92918	SUNRPC does not pass second YPBIND
CSCsg24783	FWM: With Syn cookies Syn-Ack Ack mismatched Sequence and Ack number
CSCsd86151	IF tacacs server is down first ssh connection fails
CSCsh54613	FWSM crash at route resend process
CSCsf96048	Static route with higher admin distance than OSPF route is preferred
CSCsf28989	FWSM static route config is not synchronized
CSCeh36227	Overlapping networks dont translate DNS address
CSCse70530	FWSM: high cpu and dropped connections when writing to disk: filesystem
CSCse62421	Interface IP is not re-enabled when overlapping static is removed
CSCse67618	failed conf net command resets failover commands to defaults
CSCse39175	FWSM 2.3.3.2 - crash on thread accept/http
CSCse60427	FWSM does not reboot after crashing. This caveat is equivalent to CSCee54611 in later versions.
CSCse33446	FWSM 2.3(3.6) Virtual Telnet feature First Telnet session fails
CSCsg66640	When an Object Group is edited, to apply changes ACL has to be reapplied
CSCse32037	PAT ports are not freed for outside PAT
CSCse64719	Memory leak at access_list:_create_acl_elements_og+428
CSCsg70964	2.3 : nameif causes coldstart trap
CSCse99740	When removing network objects the existing ACL lines are not removed
CSCse95070	FWSM v2.3 does not send cold start traps
CSCef27422	OSPF does not install better route upon cost change

**Table 3** Caveats Fixed between Release 2.3(4) and 2.3(5) (continued)

Caveat ID	Title
CSCsg76771	FWSM 2.3 DNS A record returns all zeros with nat exemption outside
CSCsg80240	FWSM may report being out of translation slots
CSCsh77708	Route not synced to stby if the stby ip for that intf is added later
CSCsh91836	Two dashes in name command applied to global cause break in failover
CSCsi30794	When disabling failover, state should first change to standby
CSCsi43882	Crash in 'Thread Name: lu_rx'
CSCsi45384	FWSM - duplicate udp packet causes pc conn without a valid np conn
CSCsi56801	FWM: Issuing sh pc conn causes FWSM to failover
CSCsi63155	the CPU usage of one of the context goes up to 60% and it stays there
CSCsi24174	ARP update failed at NP1 level
CSCsi35772	SMTP fixup consistently drops '250 Ok' SMTP reply
CSCsi80620	FWSM - Logging rate-limit not working correctly
CSCsj13304	FWSM - ARP Collision Syslog on Failover Sync
CSCsi31953	FWSM crash at thread telnet , while running mgcp commands
CSCsj05158	FWSM 2.3: crash displaying Thread Name: fast_fixup in dump
CSCsj22526	FWSM running 2.3.4.10 or later may stop creating new connections.
CSCsh79529	FWSM crash at Thread Name: tcp_slow

## Resolved Caveats in Software Release 2.3(4)

This section describes caveats closed in FWSM Release 2.3(4).

- CSCei49995

When using the same-security-traffic-feature and an access list applied for outbound traffic, the source IP address in the access list displayed by system log message 106023 may not be correct.

**Workaround:** None.
- CSCeg68776

With the sqlnet fixup enabled, the SQL connection is closed after 3 hours from the last SQL query even if the TCP keepalive of the Oracle server is sent.

**Workaround:** Disable the sqlnet fixup.
- CSCeh54901

With an FWSM failover pair, if one FWSM is configured with a named area ID, the other FWSM unit keeps rebooting when trying to replicate the OSPF network configuration.

**Workaround:** Before syncing the two failover units, remove the line "**name ip\_address name-A**" and change the line "**network name-A mask area name-A**" to "**network name-A mask area ip\_address.**"
- CSCsb94408

The dhcp\_daemon may crash randomly and the following error message appears on the console: An internal error occurred. Specifically, a programming assertion was violated. If this occurs, save the output of the **show version** command and the contents of the configuration file and contact Cisco TAC.

**Workaround:** None.

- CSCsd21296

When memory usage exceeds 90%, the **clear xlate** command may cause an unexpected FWSM reload.

**Workaround:** None.

The following caveats were found and fixed between Release 2.3(3.2) and 2.3(4), and were not previously documented:

**Table 4** *Caveats Found and Fixed between Release 2.3(3.2) and 2.3(4)*

Caveat ID	Title
CSCec54646	TMFW:vf_transparentMode: bad vcid (oxffffff) while booting up
CSCec89737	icmp unreachable need to fragment message not sent by FWSM
CSCee54891	show shun stats causes the FWSM to go into an infinite loop
CSCeh15390	HTTP redirect warning flag should be removed from sh np 3 vft
CSCeh34345	TFW: mac-address-table help displays optional show/clear commands
CSCeh42880	Config Error while copying from disk/tftp to running config
CSCeh63927	sysopt connection tcpmss not applied to FWSM
CSCeh66699	MGCP Fixup drops some 200 OK messages in response to an MDCX
CSCei78807	FWSM drops back to back udp packets on a new session
CSCsc03256	Modifying fixup protocol icmp at a context affects other contexts
CSCsc03377	FWSM2.3:Static routes administrative distance is shown as 0
CSCsc15401	RPC fixup sometimes does not open holes for TCP connections
CSCsc16047	FTP data session does not get replicated back to primary after failover
CSCsc19922	sysopt nodnsalias commands show up in Standby FWSM but not in Active
CSCsc22753	RTSP fixup may fail to update the TCP checksum in some circumstances
CSCsc22862	Radius Authen/autho doesn't work if user has dACL
CSCsc23710	ACL compilation with Object Groups can cause OSPF neighbor loss
CSCsc23710	ACL compilation with Object Groups can cause OSPF neighbor loss
CSCsc25427	fwsm: conn's not established after the global pool removed and readded
CSCsc27435	SM/TFW:Crash at thread accept/http
CSCsc29931	Stanby Crashes after LU_Allocate_Xlate failed messages
CSCsc33433	FWSM enable authentication issue
CSCsc33624	FWSM: Unable to send ARP request
CSCsc34709	OpenSSL Security Advisory: Potential SSL 2.0 Rollback
CSCsc35022	SQLNETfixup nonew connection allocated if oracle setup in shared mode
CSCsc49109	SKINNY: Secondary conns are not flagged

**Table 4** *Caveats Found and Fixed between Release 2.3(3.2) and 2.3(4)*

<b>Caveat ID</b>	<b>Title</b>
CSCsc51459	no nat (interface) command removes all nat statements from configuration
CSCsc53246	routes on NP1 and NP2 may get desynchronized
CSCsc58550	Ping fails on nat global and static configuration with inspect icmp disa
CSCsc60234	sh xlate inter cannot classify interfaces with same prefix name
CSCsc60567	FWSM - Thread Name: fast_fixup
CSCsc65598	SRFW: Unable to add ACE in manual commit mode
CSCsc68653	SYN cookie cause user traffic blocked
CSCsc71254	16th user ctx not getting allocated to acl partition, fws crashes
CSCsc72995	FWSM 2.3.2(21) traceback: snmp (Old pc 0x0043829a ebp 0x0f58401c)
CSCsc79063	FWSM Overlapping statics not caught when using 255.255.255.255 netmask
CSCsc80844	DHCP relay on FWSM doesn't forward Bootreply when using Bootp
CSCsc80959	Snmp getnext fails to find next interface when previous intf is deleted
CSCsc87246	NP 3 Hard assert @rm_counters.asm with traffic
CSCsc87644	Sqlnet fixup fails to create data connections in some scenarios
CSCsc89235	FWSM - Add support for new RADIUS VSA to mitigate downloadable ACL issue
CSCsc98614	FWSM crashes when creating a new context using PDM
CSCsd00407	RSH fixup closing all conns of same session, dropping FIN packets
CSCsd03945	FWSM not failover for a long time
CSCsd07178	FWSM crashes with h323_h225 thread
CSCsd07562	Traffic fails to go through from outside to inside on doing a clear conf
CSCsd13225	FWSM 2.3 Standby unit crashes in lu_rx, assertion 0 failed: file xlate
CSCsd13406	FWSM2.3:Crashes on RIP updates for same network through diff interfaces
CSCsd22977	FWSM crashing with i82543_timer
CSCsd23817	Deleting same ACE or ACL with Manual commit increment np 3 acl count
CSCsd34005	Downgrade from 3.1 to 2.3 with crypto statement causes GDB
CSCsd34005	Downgrade from 3.1 to 2.3 with crypto statement causes GDB
CSCsd34568	FWSM does not correctly order dynamic and static policy nat translations
CSCsd46335	One fixup SIP packet causes NIC stop transmitting then NIC queue sticks
CSCsd56786	FWSM 2.3.3.8 failover sync fails at update of classless IP address
CSCsd67587	FWSM: improper opening of pin-hole for SIP INFO
CSCsd75982	CLI commands when executed only output the prompt
CSCsd76039	SSL bulk depoly object group cmd may fail randomly in heavy concurrent a
CSCsd77800	Corruption caused by missing error check in ACL code
CSCsd79077	Removing ACE applied to policy-nat statement causes memory corruption
CSCsd81734	Segmented HTTP request bypasses Websense/N2H2 URL filtering
CSCsd81734	Segmented HTTP request bypasses Websense/N2H2 URL filtering

**Table 4** Caveats Found and Fixed between Release 2.3(3.2) and 2.3(4)

Caveat ID	Title
CSCsd83852	183 Response getting dropped because of no matching session
CSCsd83852	183 Response getting dropped because of no matching session
CSCsd89230	Metric for static routes wrongly displayed as 1
CSCsd90850	On Upgrade to a new image static entries are lost

## Resolved Caveats in Software Release 2.3(3.2)

This section describes caveats closed in FWSM Release 2.3(3.2).

- CSCeh66699

The FWSM in transparent firewall mode drops the first 200 OK message in response to an MGCP MDCX message. The message is retransmitted successfully.

**Workaround:** Disable the MGCP fixup using the **no fixup protocol mgcp 2427** command.

- CSCsc15401

The RPC fixup does not always correctly open holes for certain RPC connections using TCP.

**Workaround:** Configure the server to use static ports for the affected service(s). Modify the access list of the FWSM to allow traffic to these static ports.

- CSCsc16047

An FWSM with long-lived FTP sessions may not see connections replicated back to the primary FWSM after a failover event. The primary (active) FWSM will have the connection in its connection table, and the secondary (standby) FWSM will also have the connection. Upon failover, the primary unit will clear the connection table and replicate the connections from the secondary (active) unit. Some of these connections may not be replicated.

To check for this condition, enter the **show conn** command on both units before and after the failover event. The primary (standby) unit should replicate the connections within a couple of minutes.

**Workaround:** None. However, the problem will be cleared as connections terminate, and new connections will be properly replicated.

- CSCsc19922

When the standby FWSM syncs its config with the active FWSM, the first command it issues is the **clear configure all** command. This command results in the following two commands being inserted into the standby FWSM configuration:

```
sysopt nodnsalias inbound
sysopt nodnsalias outbound
```

Thus, the configurations will not be completely in sync. If a failover occurs from active to standby, then these commands will now be in effect on the newly active FWSM.

**Workaround:** Manually remove the commands on the standby FWSM.

- CSCsc22862

If you configure a dynamic access list using the Cisco ACS RADIUS server for AAA authentication or authorization, authentication or authorization fails. The FWSM sends two RADIUS access requests with the same ID number (packet ID). The time gap between these two requests is very

small, and the RADIUS server ignores the second request that requests the dynamic access list causing authentication or authorization to fail. The FWSM then marks the RADIUS server as being down.

**Workaround:** None.

## Resolved Caveats in Software Release 2.3(3)

This section describes caveats closed in FWSM Release 2.3(3) and includes the following topics:

- [AAA Caveats, page 18](#)
- [Access List Caveats, page 19](#)
- [Connection Caveats, page 21](#)
- [Routing Protocol Caveats, page 21](#)
- [System Message and SNMP Caveats, page 22](#)
- [Voice Over IP Caveats, page 22](#)
- [Miscellaneous Caveats, page 23](#)

### AAA Caveats

- CSCin88094
 

The per-user-acl override feature is configured for FTP and multiple FTP users log in from the same ip address. Sometimes when using this configuration, the per-user-acl override functionality does not work as expected when multiple FTP users connect from the same host. For example, if user\_1 is allowed FTP network access through the module and user\_2 is not, it is possible that user\_2 may have unhindered access even when per-user-acl applied to the user\_2 profile has strict network access restrictions.

**Workaround:** None, unless a restriction is in place to limit FTP users to one per host.
- CSCeh18575
 

On an FWSM in single transparent mode with the TACACS+ authentication configured, when a client passes the AAA authentication, it is denied by the **int acl** command. The log shows that the AAA authentication is denied by the wrong interface access list.

**Workaround:** None.
- CSCei90705
 

Adding more than 5,017 access control entries to an access-list tied to AAA using the AAA **match access-list** command causes the original AAA configuration statement to be removed and disables the related AAA operation. Also, upload over the network may keep the CPU utilization close to 100% for a long time.

**Workaround:** None.
- CSCei14517
 

FWSM does not support the **aaa accounting** commands, but the parser still accepts these commands.

**Workaround:** Do not use the deprecated **aaa accounting** commands.
- CSCeh71564

This applies when per-user override is enabled, TACACS+ is used for AAA authentication and authorization, and the source and destination are permitted by the AAA access list, but are denied by the inbound access list. In this configuration, during AAA authentication and authorization, the inbound access list is bypassed. After the user is authenticated and authorized, the inbound access list blocks the new session.

**Workaround:** None.

- CSCeh77632

Configuring an AAA policy and making use of an access list with more than 20K access control entries the FWSM may crash.

**Workaround:** None. Only a few thousand AAA configurations are supported, so do not configure an access list with more than a few thousand elements as in AAA configuration.

- CSCeh57549

User authentication fails when SSH to the FWSM device is enabled and users are authenticated through TACACS+.

**Workaround:** None.

## Access List Caveats

- CSCsb82279

After 16K access lists with the **log** keyword are configured on the FWSM, the message "ERROR: Unable to add access-list (rc=0xc014)" is seen on the FWSM when trying to add another access list rule containing the **log** keyword.

**Workaround:** None.

- CSCin92161

Override functionality does not work if a named access list is configured on a RADIUS server. When a user is authenticated, the dynamic access list name is displayed in the Uauth information but access the access list is not applied to traffic. Instead, the interface access takes effect and traffic is passed/denied accordingly.

**Workaround:** None.

- CSCei72714

When using an access list with access groups and using Internet Explorer to send HTTP SYN packets from a lower security interface to a higher security interface, the hit count against a deny access control entry is not accurate.

**Workaround:** None.

- CSCei56411

In access list manual commit mode, adding new members to object groups used in access lists that expand to a lot of new access control entries can result in dangling object group access control entries with an "uncommitted deletion" qualifier.

**Workaround:** Remove the object group access control entries and add them again.

- CSCei57951

Compilations in auto mode can be slow after changes have been made to large object groups tied to access lists. This may happen when back-to-back compilation is triggered.

**Workaround:** None.

- CSCei22165
 

When one or more ACEs in a file are copied using the **tftp:/disk:** command to the running configuration, the last line in the file is missed and does not get copied over.

**Workaround:** Add a dummy access control entry to the file.
- CSCei24404
 

After committing a large set of access lists, the FWSM may hang.

**Workaround:** None.
- CSCei20132
 

When using AAA authentication, authentication intermittently completely stops working without producing any traces or logs.

**Workaround:** Reload FWSM.
- CSCei10850
 

UDP packets with the source port set to 0 bypass the access rule when a destination port is also specified. An attack is possible, given an access list with a **deny udp any any eq port dest** followed by **permit any any** or **deny udp any any eq port dest** followed by **permit host attacker any**. If the attacker uses SRC port zero then the attacker can bypass the access list and reach any host on any port, including the port explicitly denied in the first access control entry. For this attack to work, there has to be a permit statement for UDP that does not specify any source or destination port (wildcarded).

**Workaround:** Use the **lt 1** port range in the access list.
- CSCeh81093
 

On FWSM Release 2.3(x), under high load conditions (more than 4000 users with downloadable access lists, the FWSM will display the following errors:

  - May 02 2005 12:08:44: %FWSM-3-109018: Downloaded ACL "username@companyname" is empty
  - May 02 2005 12:08:44: %FWSM-4-109005: Authentication succeeded for user 'username@companyname' from 10.10.10.10/4298 to 192.168.2.2/443 on interface production

At this point, all downloadable access lists appear empty. This issue is observed until the user traffic is decreased. This is the result of a hard-coded limit of approximately 4000 downloadable access lists (the exact number depends on the structure of the access list).

**Workaround:** Use the **show np3 acl count** to determine if the system is approaching the access list limit. Avoid use of repetitive downloadable access lists. Instead, used named downloadable access. Change the infrastructure so that there are fewer downloadable access lists per FWSM.
- CSCea56634
 

When FWSM Release 2.3.3 is running in single or multimode using translation or authentication rules that require access lists to define interesting traffic, the hit count in the corresponding access lists for certain functions does not increase from 0. The affected functions include NAT 0 access-list, policy NAT, policy static, crypto map match address, and AAA.

**Workaround:** None.
- CSCed62181
 

The set of access list configurations on the FWSM does not fit in the FWSM access list memory. The device tries to compile the access lists but runs out of memory while doing so. FWSM deletes all the rules added in that step automatically but the PDM/MC does not report the error and it appears as if the access list has been successfully committed.

**Workaround:** None. To monitor the access list memory usage, use the **show np 3 acl stats** command.

- CSCeg38229

The problem occurs when you perform the following steps:

1. The access list is in manual mode.
2. You configure suspend-config-sync between the active and the standby FWSM.
3. You change the access list.
4. Suspend-config-sync is then disabled.

Following the previous steps causes the access list configuration to not be synchronized between the active and standby FWSM. The access list configuration should be synchronized.

If you continue sending the **access-list commit** command, this action causes the access list to be totally out of synchronization between the active and standby modules.

**Workaround:** None.

## Connection Caveats

- CSCeh40924

When an RSH (remote shell) connection has been made to two FWSMs, the RST (reset) packet is dropped between the FWSMs. This problem can be seen when traffic must pass through multiple FWSMs.

**Workaround:** None.

- CSCei13648

When PDM sessions hang or are disconnected abnormally, or when simultaneous multiple access attempts occur to PDM, the following error may be seen: FWSM, 1550 blocks getting depleted, the low counter is reaching 0.

**Workaround:** none, except for reloading FWSM.

- CSCeh59278

After a DHCPINFORM broadcast, when a server sends a unicast reply to a client, the DHCPACK response to DHCPINFORM might get dropped by FWSM acting as a DHCP relay.

**Workaround:** Explicitly permit the communication from server (udp/67) to client (udp/68).

## Routing Protocol Caveats

- CSCei28005

When the Cisco Anamoly Guard is used with an FWSM so that the Guard sits in front of the FWSM and scrubs all incoming traffic before forwarding it to the FWSM, TCP sessions that are intercepted by the FWSM may not work. This is because the FWSM, after intercepting the SYN, sends the SYN-ACK to the Guard instead of sending it to the next hop router.

**Workaround:** Do not enable TCP Intercept on the FWSM when using it with a Cisco Anamoly Guard.

- CSCei12384

With an FWSM with multiple contexts that share a common VLAN interface, TCP RST packets do not pass two FWSM contexts. The first context receives it and correctly tears down the connection in its connection table, but the RST is not forwarded to the second context where the connection will stay idle until it times out.

**Workaround:** Change the configuration so that VLAN interfaces are not shared. In other words, route all traffic between contexts using the MSFC or an external router.

- CSCei10784

FWSM may ignore the ARP reply from certain IP address if it has a static route to the host address.

**Workaround:** None.

- CSCeh53497

If FWSM has route pointed to its interface, it does not route the packet.

**Workaround:** None.

- CSCeh51137

When there are multiple routes learned off a single interface, the network processor may fail to be updated with those routes. This prevents packets from being routed properly. Route addition (for a new next hop) may be followed by deletion of the old route.

**Workaround:** Instead of add then delete, first delete then add.

- 1CSCeh19997

With proper DSCP trust configured on the incoming physical ports and on the interface VLANs attached to the FWSM, DSCP is not being preserved when packets traverse the FWSM on a Sup720 system. This problem does not occur on a Sup2 system. This is a duplicate of CSCef71768.

**Workaround:** Configure **no mls qos rewrite ip dscp** in global configuration mode to retain the DSCP value through the FWSM.

## System Message and SNMP Caveats

- CSCei00223

When using SNMP to retrieve monitoring information, a management session cannot be established to the FWSM device.

**Workaround:** Issue SNMP queries for the interface group at least once a minute to prevent the statistics cleaner thread from expiring all entries and terminating.

## Voice Over IP Caveats

- CSCei16200

The alternative Address field does not get processed by H.323 application inspection (fixup) and the address does not get translated.

**Workaround:** None.

- CSCeh71222

SIP calls that are passing through an FWSM may fail for certain values of the CSeq number used for the call. Before Release 2.3.3, FWSM uses a signed integer for the CSeq number when tracking SIP calls. However according to RFC 3261, this value should be an unsigned integer. A message similar to the following may be seen: SIP::Error - CSeq value 12345678917 is too big.

**Workaround:** None.

## Miscellaneous Caveats

- CSCeh35392

Traffic that is using application inspection intermittently fails. The host initiating the traffic that is subject to application inspection is also accepting the connections for the traffic that is subject to the application inspection.

**Workaround:** Disable the fixups in the configuration, or change the configuration to not use the same-security.

- CSCsb76365

When issuing a command and then piping the output with the `-v` option without a subsequent parameter, the FWSM may spontaneously reload.

**Workaround:** This does not occur when a parameter is provided after the `-v` option.

- CSCsb57094

If the `show xlate` command is issued with the `interface` option, incorrect information is displayed.

**Workaround:** None.

- CSCsb35472

An FWSM in multi-context, transparent mode may drop packets to certain hosts when the traffic passes through two contexts inline. This happens when traffic goes from a higher to a lower security interface through one context and then from a higher to lower security interface in another context within the same FWSM.

**Workaround:** If failover is available, fail over to the standby FWSM then fail back to the active. This resets everything and traffic will flow again. If failover is not available, a reset of the FWSM will fix the problem.

- CSCsb36797

FWSM may reload unexpectedly when the command `debug packet interface_name ip_address netmask` is issued.

**Workaround:** None.

- CSCsb51332

This problem occurs with two Cisco Catalyst 6000s, each with an FWSM, with one configured as the active failover unit and the other as standby. FWSM is configured with two contexts on the active unit. The first context has higher security and lower security interfaces, while the second has only a lower security interface. To reach the second context on the standby unit, the packets has to go through the first context on the active unit.

Under these circumstances, if you configure AAA authentication for SSH, when you SSH to the lower security interface on the second context, packets to the first context on the active unit are denied.

- CSCei63632

When PAT is configured, the ICMP checksum for ping packets is not adjusted correctly.

**Workaround:** None.

- CSCei69396

When using FWMC to deploy a configuration that contains a line beginning with “FWSM,” the device may crash.

**Workaround:** Remove any lines in the configuration that begin with "FWSM," or comment these lines out with an exclamation point (!).

- CSCei35627

When a client on one side of a FWSM initiates a connection by sending a SYN to a server on the other side, and the server replies with an RST, the RST is silently dropped by the FWSM. The result is that the client keeps retransmitting the SYN until it times out.

**Workaround:** None.

- CSCei37067

Given an FWSM with a stateful failover, multi-context configuration, the active FWSM in a failover pair reloads randomly and produces crash information (crashinfo) where the “Thread Name” indicated is fast\_fixup. The problem occurs randomly after 2 hours and up to a few days of normal operation.

**Workaround:** None.

- CSCei02929

Using FWSM with nested object-groups (access lists) policies when memory utilization is approximately 25% will cause high CPU utilization and reloading of FWSM.

**Workaround:** Do not use the nested object-group policy. Use normal sequential network numbers (access lists) instead

- CSCei08350

When graphing in PDM with PDM history enabled, PDM fetches any historical data stored on the FWSM. The historical data stored on the FWSM has incorrect timestamps leading PDM to graph data points with incorrect times.

**Workaround:** None.

- CSCeh95463

This problem occurs when failover is enabled between two FWSM blades on the same Cisco Catalyst 6000, and FWMC is using bulk deploy and manual access list commit. FWSM closes the connection without sending any response back, which causes FWMC to fail.

**Workaround:** None.

- CSCeh56489

To clear IP address configurations for all configured interfaces on FWSM, the **clear ip** command can be used. However, if a command of form **clear ip address int xxx** is entered, the system ignores everything after **clear ip** and goes on to delete IP address configuration for all interfaces without any warning or error message.

**Workaround:** Do not enter the **clear ip address int xxx** command, which is not a valid command.

- CSCeh36227

With overlapping networks on a FWSM, the **static** (*high\_security\_interface,low\_security\_interface*) *global\_IP local\_IP mask dns* command does not convert the DNS address if the route for the overlapping network is directed to the lower security interface.

**Workaround:** Use the deprecated **alias** command to convert the DNS IP address and the lower security static (without DNS) to make the xlate work.

- CSCeh43792  
FWSM crashes with doorbell\_poll error. Not the same as CSCeg67681, even though the system network processor is hitting a hard assert in the fast path.  
**Workaround:** None.
- CSCeg79378  
In a failover pair, configured for intra-chassis failover or inter-chassis failover, the active FWSM stops forwarding packets for a few seconds when the standby unit is reloaded if **logging host** is enabled.  
**Workaround:** Disable **logging host** or remove **logging host** and **write memory** on the standby unit before reloading the standby FWSM.
- CSCeh58314  
When receiving numerous interface-related parameters simultaneously, the FWSM may exhibit high CPU utilization or unexpectedly reload when polling for the interface-related parameters.  
**Workaround:** None.
- CSCeh61359  
After applying the fix for CSCef82739, the uptime of the FWSM will not display correctly after the system has been operational for more than 49 days, 17 hours.  
**Workaround:** None.

## Resolved Caveats in Software Release 2.3(2)

- CSCed83489  
Pressing Ctrl-z while editing an item name (for example, when the cursor is in the middle of the name of the access list) causes this item to be stored together with Ctrl-z. This action will cause an incomplete configuration when booting up.  
**Workaround:** Ensure that you only use Ctrl-z on an empty line. If you encounter an incomplete configuration, copy the startup configuration to a TFTP server, inspect the configuration for the presence of the Ctrl-z characters (ASCII code 26) with the appropriate editor (one capable of showing the non-printable characters), and remove them. After correcting the problem, copy the configuration back from the TFTP server to the startup configuration and reboot the FWSM.
- CSCeg30257  
When the OSPF access lists are added in manual mode, the entries are shown as uncommitted additions and deletions, even after the commit. The access lists are not added to the Network Processor.  
**Workaround:** Use auto-mode for making any changes to the OSPF access lists.
- CSCeg29368  
After the standby FWSM reloads, it loses its SSH key.  
**Workaround:** None.
- CSCeg26735  
The system message FWSM-6-302016 does not have the byte count, duration, or interfaces associated with the connection.  
**Workaround:** None.

- CSCeg24827  
The system message FWSM-6-109025 is being erroneously displayed for secure HTTP and HTTPS users with downloadable access lists.  
**Workaround:** None.
- CSCeg23691  
When moving from single to multiple context mode on the FWSM, the object-group descriptions may not convert correctly.  
**Workaround:** Reconfigure the descriptions after enabling multiple context mode.
- CSCeg11285  
If a device is attached to the physical console port on the FWSM, there is a possibility that the FWSM will hang if certain characters are sent to the console port. The console port is an internal port on the module, and it is not accessible from the front of the module. You should not use this port without specific directions from the Cisco TAC.  
**Workaround:** Do not attach anything to the physical console port.
- CSCeg53006  
After changing the administration distance of a static route to be higher than the OSPF default administration distance, the FWSM still takes the static route. The **show route** command displays both routes.  
The expected result is after changing the static administration distance, the OSPF administration distance should take over as the preferred route. The higher administration distance static route should not display in the **show** command route table.  
**Workaround:** Pass the correct flag to account for a static route addition.
- CSCeh36792  
On a host running the FWSM device manager in transparent mode, if you configure the IP address and enter the **setup** command, the following error is displayed:

```
Switched to transparent mode Unknown interface name: Error setting the HTTP host address
```

The HTTP address is not set on the FWSM and the FWSM device manager is unable to communicate with the module.

**Workaround:** When the setup is complete, you must enter the **http ip\_addr\_of\_FWSM\_Device\_MGR mask interface** command.

- CSCef96479  
When a policy NAT is configured and a static statement already exists with the same address, the traffic goes through without a problem the first time but it will not go through a second time.  
**Workaround:** Remove the static statement.
- CSCef95396  
The **clear local** command clears the authenticated user for the traffic that has fixup enabled.  
**Workaround:** None.
- CSCef82229

With the fix for CSCef02740, the FWSM no longer displays the “I” or “O” flags in the output of the **show conn** command. These flags are used to determine if the inside host has sent a data packet (I), or if the outside host has sent a data packet (O). Without these flags, you cannot determine if a TCP data packet has been sent from either the client or server. Traffic flowing through the module is not affected.

**Workaround:** None.

- CSCef64059

The system message FWSM-3-210007 has the incorrect recommended action in the documentation.

**Workaround:** None

- CSCee85192

The system message FWSM-6-302013 and FWSM-6-302014 do not contain the interface information as described in the documentation.

**Workaround:** None.

- CSCee83391

If AAA is configured and a DOS text-based FTP program is used to FTP files, blocked files are denied by WebSense and the FWSM, but the FWSM fails to print msg 550, “550 Requested file is prohibited by URL filtering policy,” and the FTP program hangs until it times out.

**Workaround:** Do not to use an FTP text-based program.

- CSCee37328

In transparent firewall mode, if you enter the **virtual http** or **virtual telnet** command, there is a delay in establishing a connection to the virtual IP address on the FWSM.

**Workaround:** None.

## Resolved Caveats in Software Release 2.3(1)

- CSCeh06950

When upgrading from FWSM software release 1.1(3) to release 2.3(1), the failover link statements may not carry over as part of the conversion of the failover statements to a newer format. The stateful failover information number is not passed to the standby device.

**Workaround:** Remove the nameif statement for the failover link, re-configure with the correct VLAN number, and configure the **failover ip** command for the failover link.

- CSCee62030

The FWSM fails to respond after receiving invalid characters embedded in an email address contained in the SMTP inbound traffic when SMTP fixup is enabled.

**Workaround:** Disable SMTP fixup.

- CSCef28673

Two FWSMs configured as a failover bundle and running OSPF may experience problems establishing OSPF adjacencies after sequential failover sequences. This problem is diagnosed by looking at the DR/BDR status on the peer interfaces. When this situation exists, there is usually a discrepancy between the FWSM and the neighbor.

**Workaround:** Set the OSPF priority to zero or clear the IP OSPF process on the FWSM.

- CSCed83182

If a user authenticates with RADIUS for a management connection to the FWSM, and you configure a downloadable access list on the RADIUS server for the user, then the FWSM downloads the access list but fails to bind it to the user authentication session. If the user sends traffic through the FWSM while this authentication session is active, the access list will not be in effect, and the user will have unrestricted access (according to the access list associated with the interface). Also, because the access list is not bound to the session, when the session times out, the access list is not removed from the running configuration. This access list uses up the memory on the FWSM.

**Workaround:** You cannot remove this access list alone because it has a special name. You can either remove all access lists using the **clear access-list** command or reload the FWSM. To ensure authorization for users who have administrative access, we suggest that you use a TACACS+ server for authorization instead of downloadable access lists, or use the local database for CLI authentication so the RADIUS authentication is not triggered.

- CSCed83385

Virtual Telnet and virtual HTTP IP addresses are not being passed down into network processor (NP) 3. This situation causes the FWSM to not respond to ARP requests for the virtual IP addresses, and the packets directed to the virtual IP addresses are dropped.

**Workaround:** None.

- CSCee46135

For user authorization in single context mode, the FWSM does not support the downloadable access lists from a RADIUS server.

**Workaround:** Configure the access lists on the FWSM and then download the access list name from the RADIUS server.

- CSCed43330

If you configure outside NAT for a host, a SQL\*Net session through the FWSM for the host fails. The FWSM sends the local untranslated IP address of the outside host to the inside host, and eventually the session times out.

**Workaround:** Use static NAT for the outside hosts that use SQL\*Net.

- CSCee20506

The resource manager does not count more than one FTP data channel per FTP control channel, and therefore does not count any additional data channel connections toward the connection limit. Also, the **show resource usage** command does not display these connections.

**Workaround:** None.

- CSCee47998

In some circumstances, when you configure a limit on the TCP connections as well as a limit on embryonic connections in a **nat** or **static** statement, a denial of service (DoS) condition might occur. The UDP connection limits are not affected.

**Workaround:** We recommend that you configure only one of these limits at a time for a given **nat** or **static** statement, and leave the other at the default of 0 (unlimited, up to the maximum for the system). If you configure both limits, and the **show local-host** command indicates that the maximum number of TCP connections has been reached, then enter the **clear local-host** command to clear the condition.

- CSCec68302

After a unit fails over, the connections that are not actively exchanging data are not replicated back to the original active unit. As a result, if the current active unit fails over, the state of the connection is lost.

**Workaround:** None.

- CSCed51205

If you configure the active unit for manual access list commitment (the **access-list mode manual-commit** command), when the active unit replicates the configuration to the standby unit, none of the access lists on the standby unit are committed, even when they are committed on the active unit.

**Workaround:** Do not use manual commitment (set the **access-list mode auto-commit** command) on the active unit, at least while the standby unit is synchronizing the configuration. Or, after the standby unit synchronizes, enter the **access-list commit** command on the standby unit to commit all access lists.

- CSCee31514

In single context mode, the standby unit might reboot if you attempt to copy a configuration to the running configuration on the standby unit, and simultaneously enter the **copy running-config startup-config** (or **write memory**) command on the active unit.

**Workaround:** Do not configure the standby unit while you are configuring the active unit; the standby unit should get all its configuration through the replication process. Configuring the standby unit causes the units to get out of synchronization.

- CSCee47137

If you configure the failover poll and hold times (**failover polltime unit**) to be less than the default, and enable manual commitment of access lists (the **access-list mode manual-commit** command), when you commit a large access list on the active unit using the **access-list commit** command, then the failover communication is disrupted and the active unit fails over to the standby unit.

**Workaround:** Increase the failover unit poll and hold times to greater values (for example, the default of 1 second for the polltime and 15 seconds for the holdtime).

- CSCea75037

If you configure a **static** command using the **interface** keyword to specify the interface address, and if you change the interface IP address, the change is not reflected in the static translation.

**Workaround:** None.

- CSCee32145

When you configure the same security interfaces, the NAT exemption statements (**nat 0 access-list**) are ignored. You might use the NAT exemption statements to set the connection limits when you do not want to perform address translation.

**Workaround:** Use identity NAT (**nat 0**) or static identity NAT.

- CSCee48769

When you configure the embryonic limit for an inside **static** statement, and you also configure dynamic PAT for an outside interface, then a SYN attack from the outside to the inside static address causes a large number of PAT translations with the associated connections, even though the connections are not established. These PAT translations do not time out within the default 30-second interval for translations without the associated connections because the FWSM thinks there are valid connections associated. The pool of addresses and ports for the outside addresses is depleted, and no additional clients can connect.

**Workaround:** Do not configure outside PAT if you want to protect the inside address from a SYN attack using an embryonic limit.

- CSCee50131

All access lists have an implicit deny at the end consisting of **deny ip any any**. When a packet is dropped because of the implicit deny, the FWSM does not generate the system message 106023 that indicates when a packet is dropped by an access list.

**Workaround:** Add an ACE consisting of **deny ip any any** at the end of the access list. When you have an explicit ACE, you can set additional logging options as well.

- CSCin72275

When the maximum number of deny flows is reached for ACE logging, the FWSM generates system message 10601. However, if you set the alert interval for this message to be greater than the default 300 seconds, then the FWSM does not generate the message.

**Workaround:** Set the **access-list alert-interval** command to be 300 seconds or less.

- CSCec11628

Inter-cluster Cisco CallManager (3.3) trunks, connected without the use of Gatekeepers (one Cisco CallManager connected directly to another Cisco CallManager), often experience delayed or disrupted call setup and voice path connections. The majority of calls are successful.

**Workaround:** Use either Gatekeeper-controlled inter-cluster trunks, or use Cisco CallManagers on two FWSM interfaces of the same security level.

## Related Documentation

See the following sections for related documentation:

- [Hardware Documents, page 30](#)
- [Software Documents, page 30](#)

## 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*
- Catalyst 6500 Series Cisco IOS Software Configuration Guide
- Catalyst 6500 Series Cisco IOS Command Reference

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

