



# Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 4.0(x)

---

**November 2011**

This document contains release information for FWSM Release 4.0(1) through 4.0(17).



---

**Note** Release 4.0(9) is no longer available. See the [“Important Notes” section on page 2](#) for more information.

---

This document includes the following sections:

- [Important Notes, page 2](#)
- [Upgrading or Downgrading the Software, page 2](#)
- [Chassis System Requirements, page 3](#)
- [Management Support, page 4](#)
- [New Features, page 5](#)
- [Software License Information, page 8](#)
- [Limitations and Restrictions, page 8](#)
- [Open Caveats, page 9](#)
- [Resolved Caveats, page 11](#)
- [Related Documentation, page 35](#)
- [Obtaining Documentation and Submitting a Service Request, page 36](#)



---

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

© 2011 Cisco Systems, Inc. All rights reserved.

## Important Notes

- Release 4.0(9) included a caveat fix (CSCsz35702) that caused the FWSM to hang for some customers (CSCte48563) when using identity NAT. 4.0(10) is identical to 4.0(9) except that caveat CSCsz35702 remained in an open state to avoid caveat CSCte48563. Both caveats were resolved in Release 4.0(11). If you are running 4.0(9), we suggest that you immediately upgrade to 4.0(11) or later to avoid this issue.
- For traffic that passes through the control-plane path, such as packets that require Layer 7 inspection or management traffic, the FWSM sets the maximum number of out-of-order packets that can be queued for a TCP connection to 2 packets, which is not user-configurable. Other TCP normalization features that are supported on the PIX and ASA platforms are not enabled for FWSM.
- You can disable the limited TCP normalization support for FWSM using the **no control-point tcp-normalizer** command.
- When you log in to the system execution space from the switch in multiple context mode, a feature introduced in FWSM Release 3.2 lets you use authentication using a AAA server or local database. Previously, the only method of authentication available was to use the login password defined in the system configuration. The new authentication method is enabled by the **aaa authentication telnet console** command in the admin context. If you upgrade to Release 3.2 or above, and have this command already in the admin context configuration, then authentication for the system execution space is enabled using the specified server or local database, even if you did not intend to enable it. To use the login password instead, you must remove the **aaa authentication telnet console** command in the admin context.
- Do not configure both the **timeout uauth 0** command and the **aaa authentication clear-conn** command; if you do so, you cannot open any connections through the FWSM because the connection immediately closes when AAA succeeds. This happens every time you try to open a connection (because the FWSM is not caching uauth entries).
- In 3.x, when you used the **set connection** command for an access list (**match access-list**), then connection settings were applied to each individual ACE; in 4.0, connection settings are applied to the access list as a whole.

## Upgrading or Downgrading the Software

To upgrade from 2.x or 3.x to 4.0, see the “Managing Software, Licenses, and Configurations” chapter in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using the CLI*. Be sure to save a copy of your 2.x or 3.x configuration if you later want to downgrade.

After you reload the FWSM with the 4.0 image, the configuration is converted (for example, the **http-map** commands are converted to **policy-map type inspect http** commands). This converted configuration is not saved to memory until you enter the **write memory** command (or the **write memory all** command from the system execution space in multiple context mode).

If you try to downgrade using a converted configuration, many commands will be rejected. Moreover, if you add access lists to the 4.0 configuration to take advantage of larger access list memory space, then downgrading could result in an inability to load all the new access lists.

If you want to downgrade, be sure to copy a saved 2.x or 3.x configuration to the starting configuration before you reload with the 2.x or 3.x image.

# Chassis System Requirements

You can install the FWSM in the Catalyst 6500 series switches or the Cisco 7600 series routers. The configuration of both series is identical, and the series are referred to generically in this guide as the “switch.” The switch includes a switch (the supervisor engine) as well as a router (the MSFC 2).

The switch supports Cisco IOS software on both the switch supervisor engine and the integrated MSFC router.


**Note**

The Catalyst operating system software is not supported.

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.

The FWSM runs its own operating system.

This section includes the following topics:

- [Catalyst 6500 Series Requirements, page 3](#)
- [Cisco 7600 Series Requirements, page 4](#)

## Catalyst 6500 Series Requirements

Table 1 shows the supervisor engine version and software.

**Table 1** Support for FWSM 4.0 on the Catalyst 6500

Cisco IOS Software Release	Supervisor Engines <sup>1</sup>	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
12.2(33)SXI7	720-10GE	No	Yes	Yes
12.2(33)SXI7	720	No	Yes	No
12.2(33)SXJ1	720-10GE	No	Yes	Yes
12.2(33)SXJ1	720	No	Yes	No
12.2(33)SXJ1	32	No	Yes	No
12.2(33)SXJ	720-10GE	No	Yes	Yes
12.2(33)SXJ	720	No	Yes	No
12.2(33)SXJ	32	No	Yes	No
12.2(33)SXI6	720-10GE	No	Yes	Yes
12.2(33)SXI6	720	No	Yes	No
12.2(33)SXI4	720	No	Yes	No
12.2(33)SXI4	720-10GE	No	Yes	Yes
12.2(18)SXF and higher	720, 32	No	No	No

**Table 1** Support for FWSM 4.0 on the Catalyst 6500

	Supervisor Engines <sup>1</sup>	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
12.2(18)SXF2 and higher	2, 720, 32	No	No	No
12.2(33)SXI	720-10GE	No	Yes	Yes
12.2(33)SXI	720	No	Yes	No
12.2(33)SXI	32	No	Yes	No
12.2(18)ZYA	32-PISA	Yes	No	No
<b>Cisco IOS Software Modularity Release</b>				
12.2(18)SXF4	720, 32	No	No	No

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

## Cisco 7600 Series Requirements

Table 2 shows the supervisor engine version and software.

**Table 2** Support for FWSM 4.0 on the Cisco 7600

	Supervisor Engines <sup>1</sup>	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
<b>Cisco IOS Software Release</b>				
12.2(33)SRD6	720-3C-1 GE	No	No	No
12.2(33)SRA	720, 32	No	No	No
12.2(33)SRB	720, 32	No	No	No
12.2(33)SRC	720, 32, 720-1GE	No	No	No
12.2(33)SRD	720, 32, 720-1GE	No	No	No
12.2(33)SRE2	720, 720-3C-1 GE	No	No	No

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

## Management Support

The FWSM supports the following management methods:

- Cisco ASDM—Software Release 6.1F supports FWSM software Release 4.0 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

This section lists new features for each maintenance release and includes the following topics:

- [New Features in Release 4.0\(5\) through 4.0\(17\), page 5](#)
- [New Features in Release 4.0\(4\), page 5](#)
- [New Features in Release 4.0\(3\), page 6](#)
- [New Features in Release 4.0\(2\), page 6](#)
- [New Features in Release 4.0\(1\), page 6](#)

## New Features in Release 4.0(5) through 4.0(17)

There were no new features in Release 4.0(5) through 4.0(17).

## New Features in Release 4.0(4)

The following Cisco IOS-integrated features are now officially supported in FWSM:

Feature	Description
PISA integration	<p><b>Note</b> This feature depends on Cisco IOS Release 12.2(18)ZYA or later, and is only available on the Catalyst 6500 switch.</p> <p>The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type.</p>
Route Health Injection	<p><b>Note</b> This feature depends on Cisco IOS Release 12.2(33)SXI or later, and is only available on the Catalyst 6500 switch.</p> <p>Route Health Injection, or RHI, is used for injecting the connected routes, static routes, and NAT addresses configured on the FWSM into the MSFC routing table. In multiple context mode, this feature is especially valuable because of the lack of dynamic routing protocol support. The MSFC can then redistribute the route to other routing tables.</p>
Virtual Switching System (VSS) support	<p><b>Note</b> This feature depends on Cisco IOS Release 12.2(33)SXI or later, and is only available on the Catalyst 6500 switch.</p> <p>VSS is a system virtualization technology that allows the pooling of multiple Catalyst 6500 switches into a single virtual switch. If you have the FWSM installed, FWSM traffic benefits from this feature. There is no configuration on the FWSM required.</p>

## New Features in Release 4.0(3)

The SCCP (Skinny) inspection has been enhanced to do the following:

- Support registrations of SCCP version 17 phones.
- Support SCCP version 17 media related messages for opening up pinholes for video/audio streams.

The following is not supported:

- Registrations of endpoints that have IPv6 addresses. The Register messages are dropped and a debug message is generated.
- If IPv6 messages are embedded in the SCCP messages, they are not NATed or PATed; they are left untranslated.

## New Features in Release 4.0(2)

There were no new features in Release 4.0(2).

## New Features in Release 4.0(1)

[Table 3](#) lists the new features for Release 4.0(1).

**Table 3** *New Features for FWSM Release 4.0(1)*

Feature	Description
<b>Routing</b>	
EIGRP	The following EIGRP features are supported in this release: <ul style="list-style-type: none"> <li>• Summarization</li> <li>• Stub-routing</li> <li>• Route filtering</li> <li>• Manual Route summarization</li> <li>• Redistribution</li> </ul>
Static route monitoring	If you configure multiple static routes to reach a network, the route monitoring feature can detect if a network goes down so that the next best route can be used.
<b>DHCP</b>	
DHCP Option 82 support	When the switch is acting as relay agent, to interoperate with HSRP, the FWSM will preserve the Option 82 field set up by the switch.
<b>Modular Policy Framework</b>	
Inspection policy maps and class maps	The following protocols support inspection policy and/or class maps: <ul style="list-style-type: none"> <li>• DCERPC</li> <li>• ESMTTP</li> <li>• HTTP</li> <li>• SIP</li> </ul>

**Table 3** *New Features for FWSM Release 4.0(1) (continued)*

<b>Feature</b>	<b>Description</b>
Regular expressions and regular expression class maps	You can create regular expressions and regular expression class maps for use in an inspection policy map or class map.
<b>Filtering</b>	
HTTPS support with Secure Computing SmartFilter	The FWSM now supports HTTPS filtering using Secure Computing SmartFilter.
Adding the context name to Websense version 4 requests	Because Websense requests initiated from the FWSM use the pre-NATted IP address of clients, which can be overlapping, this can lead to problems in defining policies in the Websense server. Adding the context name to Websense queries lets the Websense server use the context name for policy lookups.
<b>Application Inspection</b>	
DNS Guard configurability	You can now disable DNS Guard at the CLI.
SIP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map.
HTTP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map.
ESMTP inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map.
DCERPC inspection enhancements	Numerous enhancements were added. You can now use an inspection policy map to configure special actions for inspection traffic; this method replaces the application map.
<b>Access Lists</b>	
Customizable memory partition sizes	In multiple context mode, you can change the size of memory partitions for rule use, so you can reallocate memory from one partition to another.
Rule reallocation per feature per partition	You can reallocate rules between features on a per-partition basis instead of just globally.
Access list optimization	The access list group optimization feature reduces the number of ACEs per group by merging and/or deleting redundant and conflicting ACEs without affecting the semantics of the access list.
<b>Connections and Switch Integration</b>	
Connection rate limiting	You can limit the connection rate for TCP and UDP traffic.
<b>Monitoring</b>	
New SNMP MIBs	For ACL entries and ACL hit counters (CISCO-IP-PROTOCOL-FILTER-MIB), and ARP table entries (IP-MIB).

## 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
- BGP stub support.
- GTP/GPRS support.

## Limitations and Restrictions



### Note

---

These limitations and restrictions also exist in FWSM 3.x.

---

See the following limitations and restrictions on the FWSM:

- The following features are not supported when you use TCP state bypass:
  - Application inspection—Application inspection requires both inbound and outbound traffic to go through the same FWSM, so application inspection is not supported with TCP state bypass.
  - AAA authenticated sessions—When a user authenticates with one FWSM, traffic returning via the other FWSM will be denied because the user did not authenticate with that FWSM.
- Multiple context mode does not support most dynamic routing protocols. BGP stub mode is supported. Security contexts support only static routes or BGP stub mode. You cannot enable OSPF or RIP in multiple context mode.
- 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.
- 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.

- Do not configure both the **timeout uauth 0** command and the **aaa authentication clear-conn** command; if you do so, you cannot open any connections through the FWSM because the connection immediately closes when AAA succeeds. This happens every time you try to open a connection (because the FWSM is not caching uauth entries).
- During URL filtering at high rates, the HTTP connection to the server through the FWSM might not complete correctly in some scenarios with the TCP normalizer enabled and URL filtering enabled. To solve this issue, enter the **url-block block 16** command in multiple mode or the **url-block block 128** command in single mode. (CSCsj00658)
- SIP application inspection does not match regular expressions specified in the message-path against a second or larger instance of the VIA SIP Header. Check whether your purpose is accomplished by matching the regular expression specified in the message-path against the first VIA: SIP Header. (CSCso69892)
- SIP calls with a SIP URI length greater than 256 characters are dropped by the FWSM. Make the SIP User Agent make SIP calls with a SIP URI length less than 256 characters. (CSCsm37291)
- If the FWSM uses EIGRP, and receives multiple equal-cost routes to the same destination, it installs all of them in the EIGRP topology table. But the FWSM fails to install all the equal-cost routes into the routing table. (CSCso98423)

## Open Caveats

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 4.0(1), then you need to add the caveats in this section to the resolved caveats from 4.0(2) and later to determine the complete list of open caveats.

- CSCsm66165

When an FWSM is participating in a PIM multicast network, and the FWSM has been configured to only register certain groups with the PIM RP via an access list, registration for groups might fail even though registration should be allowed. For example, the **pim rp-address** command is used in conjunction with an access list like the following:

```
access-list pim1 standard permit 209.165.200.224 255.255.255.224
access-list pim1 standard permit 209.165.201.0 255.255.255.224
access-list pim1 standard deny 209.165.202.128 255.255.255.224

pim rp-address 192.168.33.43 pim1
```

This configuration should only allow the groups associated with the 209.165.200.224/27 and 209.165.201.0/27 networks to register with the RP. However, the FWSM might fail to register these groups with the RP.

**Workaround:** Remove the *acl* argument from the **pim rp-address** command. This will allow the FWSM to register all groups with the RP.

- CSCso32645

The FWSM does not send EIGRP summarized routes under some conditions immediately after a reload even though auto-summary is enabled. This occurs when EIGRP network statements exist for 40 or more interfaces.

**Workaround:** After the reload, wait for some amount of time (depending on the number of network statements configured) and issue the **clear eigrp neighbors** command.

- CSCsr57543  
When an access list has more than one **access list remark** command, and other ACEs form an optimization scenario, one or more remark statements are removed from the optimized output.  
**Workaround:** None.
- CSCsu56609  
Voice traffic for SCCP calls does not go through when the FWSM is configured for NAT exemption (**nat 0 access-list**).  
**Workaround:** Use identity NAT (**nat 0**) or static identity NAT instead of NAT exemption. Alternatively, if the configuration allows, you can disable NAT control using the **no nat control** command.
- CSCsw44990  
The output for the **show np 3 aaa stats** command shows AAA lookup failures incrementing even though all the AAA requests are successful.  
**Workaround:** None.
- CSCsw45260  
The number of rejects shown in the **show aaa-server** command is incorrect; the RADIUS server reject counter is incrementing even though the RADIUS server is not sending any Reject messages.  
**Workaround:** None.
- CSCsy62047  
When applying an inspection service policy, the FWSM shows the following error: portmap\_index: unable to locate fixup. This occurs when the class map contains any match statements other than **match port**.  
**Workaround:** Use a class-map that matches a port or use the class-inspection-default class map.
- CSCsz82463  
The FWSM blocks certain RTSP streams.  
**Workaround:** Permit all RTSP ports.
- CSCsz95950  
ICMP Traceroute does not work across an FWSM when the traffic is routed asymmetrically between two physical FWSMs in failover. ICMP Type 11 (Time Exceeded) responses are arriving at a location that is different from the originating FWSM. This happens because the ICMP connections are not statefully replicated to the failover peer even with ICMP inspection enabled.  
**Workaround:** Do not route traffic asymmetrically; or use UDP Traceroute instead.
- CSCtc23265  
After the FWSM fails over with H.323 inspection enabled, active H.323 connections through the FWSM might be disconnected. You have to re-establish the connections.  
**Workaround:** If no NAT is being performed by the FWSM, disable the H.323 inspection and permit all necessary connectivity between the H.323 endpoints explicitly via the access lists on the FWSM.
- CSCtc73075  
With Skinny inspection enabled, some returning traffic does not get through. Therefore, phone calls only get unidirectional voice (the flow does not go through from outside to inside). This issue appears more frequently with a large number of calls.



---

**Note** This issue is not present in 4.0(2) and lower.

---

**Workaround:** None.

- CSCte69628

With a large number of ACEs configured (for example, 51,000 for single mode or 14,000 for multiple mode), if you disable access list optimization, the console might hang for 5 to 6 minutes.

**Workaround:** None. If you wait, the console will return.

- CSCte89422

When using failover, if you copy new configurations with access list and object group changes to multiple contexts simultaneously, it can result in failed synchronization to the standby unit.

**Workaround:** Copy context configurations one at a time.

## Resolved Caveats

This section includes the following topics:

- [Resolved Caveats in Software Release 4.0\(17\)](#), page 12
- [Resolved Caveats in Software Release 4.0\(16\)](#), page 12
- [Resolved Caveats in Software Release 4.0\(15\)](#), page 12
- [Resolved Caveats in Software Release 4.0\(14\)](#), page 14
- [Resolved Caveats in Software Release 4.0\(13\)](#), page 15
- [Resolved Caveats in Software Release 4.0\(12\)](#), page 17
- [Resolved Caveats in Software Release 4.0\(11\)](#), page 18
- [Resolved Caveats in Software Release 4.0\(10\)](#), page 20
- [Resolved Caveats in Software Release 4.0\(8\)](#), page 21
- [Resolved Caveats in Software Release 4.0\(7\)](#), page 23
- [Resolved Caveats in Software Release 4.0\(6\)](#), page 24
- [Resolved Caveats in Software Release 4.0\(5\)](#), page 27
- [Resolved Caveats in Software Release 4.0\(4\)](#), page 29
- [Resolved Caveats in Software Release 4.0\(3\)](#), page 30
- [Resolved Caveats in Software Release 4.0\(2\)](#), page 32
- [Resolved Caveats in Software Release 4.0\(1\)](#), page 34

## Resolved Caveats in Software Release 4.0(17)

The following caveats were resolved in Release 4.0(17) and were not previously documented. If you are a registered Cisco.com user, you can view more information about a caveat using the Bug Toolkit at the following website:

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

**Table 4** *Resolved Caveats in Release 4.0(17)*

Caveat	Description
CSCtr38044	Memory leak in 0x008881e5
CSCtr60971	Max DHCP Relay Server allowed is 10;FWSM gives error when adding 10th
CSCts38551	Fastpath NP ARP Entries not Timed Out from CP in Transparent Mode
CSCts68298	FWSM: CLI should reject multicast address for next hop IP

## Resolved Caveats in Software Release 4.0(16)

The following caveats were resolved in Release 4.0(16) and were not previously documented. If you are a registered Cisco.com user, you can view more information about a caveat using the Bug Toolkit at the following website:

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

**Table 5** *Resolved Caveats in Release 4.0(16)*

Caveat	Description
CSCsk71402	fwsm - cannot add static mac-address-table entry
CSCso92808	CUPC fails to transmit port 50001 due to reassembly limit of 8192
CSCtb31446	fast path NP Hard assert causes FWSM to pause indefinitely
CSCti25015	route-monitor: inconsistency of metric after second gateway recovery
CSCti93353	FWSM dns doctoring might over-write embedded ip addresses it should not
CSCtj31001	FWSM does not pass Jumbo IPV6 packets
CSCtl01291	FWSM 3.2 - deny-flow-max stuck when denied is not at 4096
CSCtl06095	FWSM allowing some tcp non-syn pkts to pass when there is no conn
CSCtl76091	Issuing commands for mcast displaying the same database crashes FWSM.
CSCtl92927	crash at 0xb5b9f2 in Thread name ssh
CSCtn83135	NAT failure for data channel connections in Transparent FW mode
CSCto56305	FWSM nested traceback in thread name doorbell poll (NP2 PC 0x5ba1)

## Resolved Caveats in Software Release 4.0(15)

The following caveats were resolved in Release 4.0(15) 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](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 occurred.

**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 be found at the following URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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://www.cisco.com/warp/public/707/cisco-sa-20110223-fwsm.shtml>

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://www.cisco.com/warp/public/707/cisco-sa-20110223-asa.shtml>

## Resolved Caveats in Software Release 4.0(14)

- CSCtj18748
 

When the FWSM is in single mode and running Version 4.0.11 or later, output of the **show version** command may show “<system>,” even when in single context mode.

**Workaround:** None. This situation is cosmetic only.
- CSCtj21761
 

In all versions of FWSM in major builds 3 and 4, the **term pager ##** command in privileged EXEC mode changes the pager for all current sessions and future sessions. According to the purpose of this command, it should only affect the session in which it is run.

**Workaround:** None.
- CSCtj29249
 

When you have an FWSM with TCP state bypass configured, the FWSM does not send back an RST-ACK packet when it receives a non-syn TCP packet that does not match a currently-established connection. We are seeing many of syslogs, such as 106015 - “Deny TCP (no connection)” for endpoints, related to this connection.

The FWSM should be sending a RST-ACK back to this endpoint to have it open a NEW connection with a SYN. Instead, the client never gets a RST-ACK and continues to retransmit before opening a new connection.

**Workaround:** Remove the TCP state bypass configuration.
- CSCtj46839
 

When you try to perform RTSP streaming from SonyEricsson K801i and C702, and so on, then FWSM does not open pin holes.

**Workaround:** Define the specific routes for client and server for a bridge group.
- CSCtj62348
 

When the configured interface is removed on FWSM version 4.1.2 the **management-access** command is left behind and incomplete if the interface configured for management access is removed. This orphaned command cannot be removed using the **no** form of the command.

This condition may exist on other software builds, as well.

**Workaround:** Remove the management access configuration with the **clear configure management-access** command.

- CSCtj78005

When state-bypass was configured at one time and had been removed from the configuration, FWSM does not log the Deny TCP no connection or send RST back for a non-syn TCP packet.

**Workaround:** Ensure that state-bypass is not in the startup-configuration, and reload the FWSM.

- CSCtk19326

When an FWSM is running Version 4.0, and the **service reset no-connection** command is configured (in admin context if multi-mode), then the FWSM does not send RSTs back to the host for outbound non-syn TCP segments when no connection exists.

The following is sample output from the **show np [1|2] global-table** command:

```

  \- Tcp Reset Enabled: 0

0 = do not send RST
1 = send RST

```

**Workaround:** Remove and reapply the **service reset no-connection** command.

- CSCtk62630

When you enter the **copy optimized-running-config** command on an FWSM with optimized ACLs, the resulting ACL copied into the running-config is corrupted and missing large portions.

**Workaround:** Do not run the **copy optimized-running-config** command. This command serves only to copy the optimized ACL back into the running configuration. It is not required for ACL optimization to function.

- CSCti41683

When you have two separate class-maps configured, one for “application inspection” and the other for “tcp-state-bypass” with deny ACEs for traffic that need “application inspection,” though the traffic hits the deny ACE for the class-map whose action is “tcp-state-bypass,” the same traffic still does not pass through any other application inspection configuration leading to protocols like FTP, which need dynamic ports to be opened to not work.

**Workaround:** Either open all ports for the hosts that need application inspection, which is a security concern, or remove the tcp-state-bypass configuration, both of which might lead to connectivity issues.

## Resolved Caveats in Software Release 4.0(13)

- CSCsu64376

The standby device reloads when you add TCP to an object group within an access list in port 0.

**Workaround:** Do not use port 0 for TCP.

- CSCtf84419

Multiple policy NAT statements might not match right until you recompile the ACL. If you configure two policy NAT statements that overlap, and the first policy NAT ACL uses object groups, when a second policy NAT statement is added that overlaps (the ACL could also match the traffic but is less specific), the xlate is built using the new NAT entry.

**Workaround:** Edit either one of the policy NAT ACLs in any way and then recompile. The problem disappears.

- CSCth49514

When FWSMs are configured for failover mode with dynamic NAT, and failover is triggered after a considerable amount of dynamic NAT xlate's have been created or deleted, an error message appears on the newly-formed active blade.

**Workaround:** Entering the **clear xlate** or **clear local-host** can resolve the issue.

- CSCth72685

A “FWSM np completion-unit disabled” operation that is performed after reboot is not activated; however, it appears in the startup configuration.

**Workaround:** Disable and enable again after startup.

- CSCth86890

Performing an snmpwalk on the admin context shows only the failover IP address in the “ipAdEntAddr” table.

**Workaround:** Use another context to perform the snmpwalk.

- CSCti38339

When the FWSM is running Version 4.0(x) with skinny inspection enabled, FWSM may reload with traceback in Thread Name: skinny.

**Workaround:** Disable skinny inspection.

- CSCtc23265

This caveat communicates a change to the way the firewall handles flows (after a failover) that are subjected to the TCP proxy.

The TCP proxy feature on the firewall is active for connections that require higher-level inspection. For example, if the inspection engines are enabled for certain traffic flows, such as SQLnet or voice signalling traffic, the TCP proxy feature on the firewall ensures that the firewall receives the complete TCP data to perform complete traffic inspection.

This code change implements a change whereby if a failover takes place as the active firewall is processing TCP traffic subjected by the proxy. When the old standby firewall becomes active, it will update the state of the TCP connection when traffic is received on that TCP. Therefore, it will update its TCP state for the connection according to the traffic received from the TCP endpoints, and the TCP connection should continue to flow correctly.

Before this change, if a failover occurred while the firewall was processing traffic subjected to the TCP proxy, the new active firewall might not have an up-to-date connection state for that TCP, causing the firewall to send inappropriate ACKs to the TCP endpoints and to update their TCP state to match that of the firewall. This situation could cause a storm of traffic, as the firewall and the TCP endpoints both try to update each other with their version of the “correct” TCP state, the CPU on the firewall might be high, and the connectivity through the firewall for these flows might suffer.

**Workaround:** None.

- CSCth51877

When you try to log into the FWSM through SSH when primary TACACS fails, the first try always fails.

**Workaround:** Reconnect after the failure, and log in again. The second try succeeds.

- CSCth64565

In FWSM Version 3.2(10), entering the **sunrpc-server** command will only work with /32 masks defined if using Server IP host. If you want to use the network mask, then you need to define the network IP. If you are using the Server IP address and the network mask, it will not work. It will not trigger the sunrpc-server.

**Workaround:** Define mask /32 is using Server IP host. Define network IP is using network mask

- CSCth95284

A FWSM that running Version 4.0(11) might crash at Thread Name: PAT XlateCache.

**Workaround:** None.

- CSCti12787

After you upgrade an FWSM from Version 4.0(8) to Version 4.0(12) in an IPV6 environment, the CPU usage is high, about 99%.

**Workaround:** Temporarily downgrade to Version 4.0(8). The CPU usage should return to the normal baseline usage.

## Resolved Caveats in Software Release 4.0(12)

- CSCtc54126

When using SIP inspection, the connection table continuously increases with stuck SIP media connections. The SIP inspection does not clear them automatically.

**Workaround:** Enter the **clear xlate** command to clear all connections.

- CSCtf83964

With failover enabled, OSPF takes a long time to reach fully loaded state with OSPF neighbors.

**Workaround:** Use static routes.

- CSCtf87102

When you have a large number of access lists (over 100,000) and access-list optimization is enabled, access lists may not compile as expected.

**Workaround:** Disable access-list optimization.

- CSCtf94490

The **snmpget** command is failing for the following parameter:

CISCO-UNIFIED-FIREWALL-MIB::cufwUrfServerStatus

snmpwalk responds back with a value, but snmpget fails for the same OID.

For example:

```
# snmpwalk -On -v 2c -c SEGE sdhq-fwm-02-01
.1.3.6.1.4.1.9.9.491.1.3.3.1.1.5

.1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.1.4.10.80.24.103.15868 = INTEGER:
online(1)

# snmpget -v 2c -c SEGE sdhq-fwm-02-01
.1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.1.4.10.80.24.103.15868

CISCO-UNIFIED-FIREWALL-MIB::cufwUrfServerStatus.ipv4."10.80.24.103".158
68 = No Such instance currently exists at this OID
```

**Workaround:** Use snmpwalk instead of snmpget.

The caveats listed in [Table 6](#) were resolved in software Release 4.0(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 6** *Resolved Caveats in Release 4.0(12)*

Caveat ID	Description
CSCsf01863	Syslog 302013 does not show user field properly
CSCtd94681	FWSM re-uses some PAT translation ports too frequently
CSCte49110	FWSM setting DF bit on reassembled skinny packet
CSCte85951	Memory leak with HTTP inspection and “match” commands in policy-map
CSCtf15459	FWSM: about 15 seconds continuous traffic drops when active is reloaded
CSCtf31676	Secondary Active FWSM Creates a Context Using BIA MAC
CSCtf41503	FWSM sends a ACK with wrong TCP options.
CSCtf51696	SQL*Net Inspection Opens Pinholes Based on Non-Redirect Messages
CSCtf57135	fws 3.2 - deny-flow-max stuck when denied is not at 4096
CSCtf73798	CheckHeaps crash after SSH command
CSCtf77950	SNMP - Interfaces not recognized by snmpwalk to FWSM
CSCtf92566	IPv6 fragment packet dropped with “Invalid udp length”
CSCtg01772	FWSM stops traffic forwarding by changing static route's distance metric
CSCtg14948	FWSM DHCPrelay intermittent failures
CSCtg17279	In shared vlan scenario destination NAT might break communication.
CSCtg31044	client_port field is not rewritten in the RTSP SETUP reply
CSCtg35889	NP1/2 Lockup on standby FWSM
CSCtg60275	Configuring conflicting static NAT causes failover fail and sync config
CSCtg64606	Some Special IPV6 addresses can not be handled by FWSM well
CSCtg66395	FWSM doesn't NAT Audio stream of SIP connection
CSCtg91966	Unicast RPF statistics cannot be cleared.
CSCth10381	FWSM: Discrepancy between sh perfmon vs sh service-policy output
CSCth48464	Secondary Pinhole not opened for SDP two-media connections

## Resolved Caveats in Software Release 4.0(11)

- CSCsz35702

When the FWSM is configured for PAT with failover, and you force a failover, then the portmap translation fails (syslog message 305006 appears).

**Workaround:** None.

- CSCtd19411

If an additional firewall (such as the Cisco ASA 5500 series or another FWSM) is between a client and a transparent mode FWSM, then cut-through proxy/network authentication fails:

```
client ---- ASA --- FWSM (transparent mode/cut through proxy) --- cloud
```

**Workaround:** Disable TCP-state checking on the intermediate device (the “ASA” in the above example) by configuring TCP state bypass, or move the client to the directly-connected inside interface of the FWSM.

- CSCtd23101

The access list optimization feature causes missing access-list entries. It appears that the problem is triggered when there is a combination of merge up and merge down access-list rules.

**Workaround:** Disable the access-list optimization feature using the **no access-list optimization enable** command. Otherwise, a potential workaround is to avoid a merge up + merge down by arranging the order of the entries.

- CSCtd46324

With DNS guard enabled, the FWSM software sometimes reloads while deleting a DNS session.

**Workaround:** Disable DNS guard using the **no dns-guard** command.

- CSCsz81503

Multicast bidirectional forwarding fails on the FWSM due to an incorrect forwarding entry, which can be seen with the **show np 3 mroute** command. This problem can be seen when using OSPF in redundant FWSM environments where the FWSM is between the multicast source and the RP. This problem was not reproducible with a single FWSM.

**Workaround:** Enter the **clear ospf process** command.

- CSCtc38617

The TCP Sequence Number Randomization feature is not disabled on packets injected into a TCP State Bypassed connection from an interface other than the original pair and destined to a higher-security interface.

**Workaround:** None.

- CSCte71019

In failover, if you change the access list mode from manual commit to auto commit, the standby unit starts to compile the access lists again, and experiences high CPU.

**Workaround:** None.

The caveats listed in [Table 7](#) were resolved in software Release 4.0(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 7** Resolved Caveats in Release 4.0(11)

Caveat ID	Description
CSCtd42763	FWSM: Syslog 111005 does not print when exiting config mode
CSCtd60672	FWSM fails to compile ACL when custom partition size used with failover
CSCtd62290	FWSM: TACACS+ CMD Accounting packets have a Caller-ID field of 0.0.0.0
CSCtd72287	FWSM: unexpectedly reloads in Thread Name: MGCP
CSCtd78604	FWSM: ACLs missing after adding items to object-groups

**Table 7** *Resolved Caveats in Release 4.0(11) (continued)*

Caveat ID	Description
CSCtd86296	FWSM: Need to extend syslog message %FWSM-2-106024
CSCte25307	Telnet NOOP command sent to FWSM causes next character to be dropped
CSCte48165	Broken single ip address feature for more than 1 “virtual” protocols use
CSCte48563	NP3 pauses due to duplicate xlate created for identity traffic
CSCte51034	FWSM doesnt failover static routes pointing to its own interface
CSCte66339	policy-map names exceeding 16 characters leak memory upon ACE addition
CSCte70411	IPv6 object-group does not allow nested objects
CSCtf49704	FWSM software forced reloads in - Thread Name: websns_snd

## Resolved Caveats in Software Release 4.0(10)

- CSCtb34170  
 When the FWSM is configured with a static PAT command on the outside interface, if you remove the command, traffic from inside to outside is blocked. This occurs even when **nat-control** is disabled. To recover, you need to reload the FWSM.  
**Workaround:** None.
- CSCtc36380  
 The FWSM corrupts the ICMP checksum of ICMP unreachable traffic that passes through the FWSM. This causes the destination host to discard the packet because the checksum is not correct.  
**Workaround:** None.

The caveats listed in [Table 8](#) were resolved in software Release 4.0(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 8** *Resolved Caveats in Release 4.0(10)*

Caveat ID	Description
CSCsk12223	FWSM running 3.1.6 crashes on Thread name ssh
CSCta64836	Firewall blade unexpectdly reloads with traffic
CSCta64957	No new connections on after failover with a particular NAT configuration
CSCta74788	Incorrect xlate replicated to standby for same security interface
CSCtb14966	SunRPC inspection drops GETPORT reply packet
CSCtb34170	Static PAT causing failure for traffic from inside
CSCtc02363	RTSP inspect incorrect IP address translation in URL headers
CSCtc36009	TCP reset option incorrectly appears in set connection timeout command
CSCtc36050	capture feature shows ICMP payload modified by firewall when it is not
CSCtc40207	Standby transparent FWSM might send arp request using active MAC
CSCtc68193	snmp query for any OID under 1.3.6.1.2.1. causes np xlate query

**Table 8** Resolved Caveats in Release 4.0(10) (continued)

Caveat ID	Description
CSCtc71533	IPv6 object-group does not allow group-objects
CSCtc72148	WS-C6506-E-FWM/ High CPU usage
CSCtc97643	Traffic gets drop when acl optimization is on and after modifying ACEs
CSCtd04061	IMPORTANT TLS/SSL SECURITY UPDATE
CSCtd33652	virtual console hang in optimization
CSCtd73676	Only one virtual protocol can be configured with the “virtual” command

## Resolved Caveats in Software Release 4.0(8)

- CSCsy28731

The capture output of inspected traffic is not readable.

**Workaround:** None.

- CSCta73803 (see also CSCtb62411)

In multiple context mode, the FWSM might experience a depletion in the 16384 byte blocks if multiple contexts are subjected to SNMP polling simultaneously. Once in this condition, you must reload the FWSM.

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

For example:

```
hostname# 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 the **show blocks old | begin 16384** command will show output relating to SNMP:

For example:

```
hostname# 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.
- CSCtb49822
 

Some web pages with long URLs (the length of the URL is greater than 1159 bytes) might fail to load through the FWSM when it is configured for URL filtering. This occurs when the HTTP GET is segmented across multiple TCP packets by the HTTP client, and the HOST portion of the HTTP request is not present in the first TCP packet of the GET request. This might occur with Internet Explorer, but not with Firefox.

**Workaround:** To mitigate this problem, do one or more of the following:

- Add the **longurl-truncate** argument to the **filter** command. For example:
 

```
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 longurl-truncate
```
- Use Firefox instead of Internet Explorer.

The caveats listed in [Table 9](#) were resolved in software Release 4.0(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 9** *Resolved Caveats in Release 4.0(8)*

Caveat ID	Description
CSCtb03565	FWSM corrupts ICMP time to live exceeded with MPLS TAG
CSCtb18847	NP 3 pause indefinitely with established command
CSCtb23513	Authentication in progress sessions not removed with DACLs
CSCtb29859	NP hang where NP 3 fails to communicate with NP1/2
CSCtb49352	FWSM Cert Enrollment doesn't work with SCEP
CSCtb76719	Meaning of Flags 's' and 'S' is Reversed in 'show conn detail' Output
CSCtb88893	Transparent mode FWSM, Active passing broadcast arp from standby
CSCtc12597	FWSM software forced reload in Thread Name: ACL Cache during SNMP Poll
CSCtc36651	FTP fails in Active/Active mode when two contexts not active on same FW

## Resolved Caveats in Software Release 4.0(7)

- CSCsy18657

With SCCP V17, the FWSM becomes inaccessible when dual stack or IPv6 traffic passes through.

Call flow:

Phone A (dual stack) --> FWSM --> CUCM (dual stack) --> FWSM -- Phone B

When Phone A calls Phone B via the FWSM and CUCM, the FWSM unexpectedly reloads.

**Workaround:** Remove the dual stack or IPv6 configuration on the Phones and CUCM.

- CSCsz20693

The FWSM unexpectedly reloads with a high RTSP traffic load when RTSP inspection is enabled. This occurs with a large amount of RTSP traffic, around 42K connections/sec including RTSP traffic through the box. This software reload is not seen with a single RTSP connection.

**Workaround:** Disable RTSP inspection or reduce the amount of traffic.

- CSCsz92926

When trying to distribute a large number of GLOBAL lines into OSPF on an FWSM, the OSPF process may stop processing new LSAs and no longer update the routing table of its peers.

**Workaround:** If possible, summarize the routes you are trying to distribute, thereby decreasing the load on the OSPF process.

The caveats listed in [Table 10](#) were resolved in software Release 4.0(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 10**      **Resolved Caveats in Release 4.0(7)**

Caveat ID	Description
CSCtb18628	Route-monitor not update the routing table with same metric routes
CSCta44620	Software forced reset in fast_fixup with multiple FTP connections
CSCta68828	FWSM forming OSPF adjacency with 5 seconds delay
CSCsh70585	ERROR message doesn't say reason for acl insertion failure
CSCta58702	FWSM pause indefinitely due to high icmp traffic through 2 met sessions
CSCta60764	Cut-thru-proxy:certificate error after completion of initial authentication
CSCta83188	Syslog 111008 doesn't display the subnet mask with the network-object cm
CSCta58464	FTP data connection times out
CSCta62033	Adding remark lines to an optimized ACL can trigger prolonged high CPU
CSCta64995	# (hash) is lost from per-host snmp-server community after bulk sync
CSCta77829	ACL hitcount not updated in ASDM and in show access-list brief
CSCta47271	Software forced reset after enabling 'debug sunrpc'
CSCta17569	local-host objects not being freed.
CSCta41216	Login successful window closes straight away on HTTP cut through proxy
CSCta08654	Intface in shut down status intercepts traversing traffic

**Table 10**      **Resolved Caveats in Release 4.0(7) (continued)**

Caveat ID	Description
CSCta13098	FWSM sends TCP RST with wrong ACK nbr
CSCta06559	Inspect SIP shows error “portmap_index: unable to locate fixup”
CSCsv22070	Logging to the console causes syslog to be rate-limited.
CSCsz79758	H.323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT
CSCsz75402	TCP checksum errors after failover for new connections.
CSCsz68425	Transparent FWSM not Sync'ing Valid CAM Table Entries to Failover Peer
CSCsz66958	FWSM should send gratuitous ARP if new Primary inserted in failover
CSCsz66760	snmp-server enable traps command appears in the standby FWSM
CSCta10823	In certain case ACE limit reached error is not appearing in Manual mode

## Resolved Caveats in Software Release 4.0(6)

- CSCsu01658

If you configure an access list allowing TFTP and attach it to a **capture** command configured on an interface, then for a TFTP file transfer, the capture output shows that the transfer is happening to an incorrect port on the client. Also, the size of the transferred file is not shown properly.

**Workaround:** None.
- CSCsx63737

When the Auto Update Server has an action such as a replace or merge, it does not receive the Next poll message. In the output of the **show auto-update** command, “Next poll” information is missing even after waiting for more than 3 minutes.

**Workaround:** None.
- CSCsx64037

When you configure the **logging ftp-bufferwrap** command, the FTP process might stop working after a period of normal operation. This happens when the FTP server is not able to open the data connection during the active FTP transfer. The FWSM FTP process will sit idle indefinitely.

**Workaround:** Reload the FWSM, or enter the **logging host** command instead of **logging ftp-bufferwrap**.
- CSCsy09769

If you configure a policy static NAT statement with an access-list with the protocol of icmp and an icmp-type of echo, then when you ping through the FWSM, a static xlate is not created.

For example:

Inside PC (10.2.1.1) -----FWSM-----Outside PC (10.1.1.65)

```
access-list test permit icmp host 10.2.1.1 any echo
access-list test permit icmp host 10.2.1.1 any echo-reply
static (inside,outside) 10.1.1.68 access-list test
```

Then when you ping from 10.2.1.1 to 10.1.1.65, a static xlate is not created.

**Workaround:** Add an ACE without the ICMP type specified.
- CSCsy42935

SNMP polling when a user deletes an access list in manual mode causes 99% CPU and a nonresponsive console on the FWSM. When the FWSM console is nonresponsive, the following messages are seen continuously in snmp-polling pc:

```
SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.110.101.119 = INTEGER: 2
```

```
SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.97.108.112 = INTEGER: 2
```

**Workaround:** Change the commit mode to auto using the **access-list mode auto-commit** command.

- CSCsy60652

Occasionally, the FWSM unexpectedly reloads when you enter the **show failover history** command.

**Workaround:** None.

- CSCsy66470

The snmpwalk fails when the SNMP agent on the FWSM sends the response in a non-lexicographical order.

**Workaround:** Use the -Cc option while doing a snmpwalk.

- CSCsy68869

In transparent mode, snmpwalk on the TCP and UDP MIB does not display all the connections in the connection table.

**Workaround:** None.

- CSCsy84408

In some cases, the route-monitor uses the route metric of a previously configured route instead of the present metric.

**Workaround:** Configure the static routes first and then add the **route-monitor** command.

- CSCsy86901

In a same-security inter-interface configuration, NAT is not required. But for connections to virtual Telnet/HTTP/SSH IP addresses between same-security interfaces when NAT control is enabled, if the NAT configuration is absent, the FWSM fails to create the connection. You see the following syslog message:

```
%FWSM-3-305005: No translation group found for tcp src inside:<ip>/37249 dst outside:<ip>/23
```

**Workaround:** Disable NAT control using the **no nat-control** command, or configure NAT for the virtual IP addresses.

- CSCsz19454

Syslog message 106100 does not show the correct access list hit count. When logging is enabled for the access list, and the access list is hit by the first packet, the syslog message shows the correct hit-count as 1, but on subsequent hits, the syslog message does not increment the access list hit count. It always shows the hit-count as 1.

**Workaround:** To see the correct hit count, enter the **show access-list** command.

The caveats listed in [Table 11](#) were resolved in software Release 4.0(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 11** *Resolved Caveats in Release 4.0(6)*

<b>Caveat ID</b>	<b>Description</b>
CSCsl68060	Traceback in Thread Name: OSPF Router
CSCsm96999	Saving a config to disk;,"sh disk:" and "dir" gives diff saved times
CSCsq39801	FWSM syslog message report negative number
CSCsr68825	Failover: FWSM should not send TCP RST unless it is Active
CSCsr73708	FWSM/NP3 all threads stuck at address 0x3300
CSCsr99226	Static PAT w/ACL on FWSM silently drops unmatched traffic
CSCsv27205	FWSM - access-group are bypassed if source address is Class E
CSCsv31759	Applying a service-policy to an interface affects the global policy
CSCsv71697	Flags of xlate made by outside policy NAT incorrect in standby
CSCsv73391	fwsM might drop multicast traffic with a static default mroute
CSCsx75701	FWSM log 106101 triggered but max flows not reached
CSCsx97979	ENH show np x thread - should display all thread output
CSCsy01150	Show service-policy flow tcp command is broken
CSCsy34261	FWSM: 256 blocks get depleted by syslog messages
CSCsy34495	Incomplete dhcprelay config makes a valid one fail
CSCsy35054	NP1/2 UDP conns not updated when MAC address changes
CSCsy69895	Traceback in thread: sip
CSCsy88893	Should warn about impossible next hop of static route
CSCsy95843	FWSM Traceback in fast_fixup
CSCsy97933	NAT exemption and dynamic NAT conflict between same-security interfaces
CSCsz22099	xlate on shared interface causes bad connection with high data rate
CSCsz23283	FWSM responds to snmpwalk in non-lexiographical order
CSCsz31082	copy optimized run can cause larger config size than 3mb limit
CSCsz47735	FWSM doesn't support H.323 with VCON MXM 4.7 and XPoint 7.500.062
CSCsz49945	copy flash:startup-config tftp traffic passing through the user context
CSCsz51960	Traceback with Thread Name: fover_ifc_test on standby module
CSCsz57041	Inconsistent behavior in adding access-list remark in manual-commit mode
CSCsz73675	FWSM software forced reloads in ssh thread during dhcprelay config
CSCsz92982	multicast connections show bogus vlan number

## Resolved Caveats in Software Release 4.0(5)

- CSCsu69518

Even though SCCP inspection drops the registration message for phones containing IPv6 addresses (dual mode), the FWSM creates an entry for the SCCP phone as seen in the **show skinny** command output. This entry is not cleared until the FWSM is reloaded. After the registration message is dropped, if the phones keep retrying for registration, then a large number of entries are created for these phones that do not get cleared. Eventually when a large number of false entries are created, the FWSM will be unable to add further entries for phones that try to register later.

**Workaround:** None.

- CSCsw46905

When using Active/Active failover, during configuration replication, the active FWSM might unexpectedly reload. When the reload occurs, the FWSM becomes unresponsive.

**Workaround:** To reset the FWSM, enter the **hw-module module module\_number reset** command at the switch CLI, or power cycle the FWSM in configuration mode by entering the **no power enable module module\_number** command, then the **power enable module module\_number** command.

- CSCsx09390

When you have an FWSM Active/Active failover pair, with one in an active VSS switch and the other in the standby VSS switch, then if you shut down the FWSM failover VLAN on the active switch and then enter **redundancy force-switchover** on the switch, you cannot session to FWSM on the standby switch from the active switch.

This issue also occurs if you shut down the failover VLAN, and then reload the FWSM in the active switch.

This issue also occurs if you change from VSS to standalone, and then back to VSS.

**Workaround:** For the two conditions associated with shutting down the failover VLAN, enter **no shutdown** for the FWSM failover VLAN on the active switch. For the condition related to changing from VSS to standalone, then you need to disable failover on both FWSMs by entering **clear configure failover** on the standby unit, and **no failover** on the active unit after you change from VSS to standalone. After you change back from standalone to VSS, you can reenabling failover.

- CSCsx41274

When using route health injection, if you perform an SSO switchover on the switch, followed by a failover of FWSMs, static routes associated with the FWSM are not seen on the newly active switch.

**Workaround:** Remove the **route-inject** command from the newly active FWSM and re-add it. Static routes will then get populated on the switch.

The caveats listed in [Table 12](#) were resolved in software Release 4.0(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 12**      **Resolved Caveats in Release 4.0(5)**

Caveat ID	Description
CSCeh90462	FWSM silently drops TCP SYN while cleaning up old connection
CSCsg87042	FWSM : Backspace character counts as return for enable password
CSCsi30615	show version output shows: Int: Not licensed

**Table 12** *Resolved Caveats in Release 4.0(5) (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCsk05321	'show connection detail' should show true interface names
CSCsl63063	FWSM - unexpected reload in thread doorbell_poll: NP2 / PC 0x3a1a
CSCso06871	FWSM 4.0 : Uncomment fast path syslog code
CSCsu21962	FWSM unexpectedly reloadsin Thread Name: doorbell_poll or Syslog_entry
CSCsu26449	FWSM: Smart Filter URL filtering may break - FWSM may send reset
CSCsu46215	H.323 communication fails through FWSM with tcp-normalizer enabled
CSCsv14944	FWSM unexpectedly reloads in Thread Name: doorbell_poll 0x3cec NP1 / NP2
CSCsv27205	FWSM - access-group are bypassed if source address is Class E
CSCsv41010	FWSM unexpectedly realods at thread name udp_sip
CSCsv42245	HTTP traffic not going through with routed ASR topology
CSCsv46585	Modifying an ACL can cause traffic to be incorrectly allowed
CSCsv82747	Bitmap corruption after switchover
CSCsv83322	FWSM 'Who' Command is Locked in Configuration Mode
CSCsv90335	Traffic not Sent to Original Context with ASR Groups Configured
CSCsv91984	Remove Warning message when enabling sysopt np completion-unit
CSCsw17796	FWSM access-group is not automatically updated for an ipv6 access-list
CSCsw40164	Failover interfaces should be in the ipAddrtable (extend CSCsl29965)
CSCsw46905	Traceback in fover_parse thread - CLI entered on Primary
CSCsw77676	FWSM: No logging message 710003 does not work
CSCsw79372	Fwsm 3.2 might stop processing incoming ospf hellos on some interfaces
CSCsw93154	DHCP-relay packets to PC dropped due to multicast traffic pressure
CSCsx00376	FWSM: May unexpectedly reload in Thread Name: fover_parse
CSCsx08762	ENH: Established entries in CP and NP go out of sync for sunrpc traffic
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
CSCsx41093	NP-PCmplx logger frame timeout with SNMP Polling
CSCsx44248	Area in network ospf command cannot have a name
CSCsx54892	Non-standard log message format %FWSM--1-710002
CSCsx59229	Standalone 'Failover' Command Stops All Local Outgoing Traffic
CSCsx66450	index value is incorrect when individually run snmpget for each ifindex
CSCsx82996	Traceback: doorbell_name
CSCsy00911	Abnormal Consumption of 56 and 80 Byte Memory Segments with Logging Mail
CSCsy03439	FWSM: SNMP coldstart trap not sent in failover scenario
CSCsy06702	FWSM - virtual http x.x.x.x may disappear from the config after a reboot
CSCsy26815	Transparent FWSM treats uncorrectly fragmented inspected h.323 packet

**Table 12** *Resolved Caveats in Release 4.0(5) (continued)*

Caveat ID	Description
CSCsy30199	Memory leak with HTTP inspection and HTTP map applied
CSCsy43127	FWSM 4.0 : ACE mibs snmp polling causing high cpu and unexpected reload

## Resolved Caveats in Software Release 4.0(4)

- CSCsv00658

Access list optimization might create an access list that is inaccurate compared to the original access list. This may cause packets to be denied when they should be permitted by the access list.

**Workaround:** Disable access list optimization with the **no access-list optimization enable** command.

The caveats listed in [Table 13](#) were resolved in software Release 4.0(4), 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** *Resolved Caveats in Release 4.0(4)*

Caveat ID	Description
CSCsl16482	HTTP authentication with ssl trust-point is not working after reload
CSCsm90200	FWSM show memory displays incorrect data in multi context mode
CSCsq27152	ASDM location commands do not appear in show run all output
CSCsr91871	GTP: SGSN context request/response trigger errors
CSCsr93879	GTP: identification request/response trigger packet parsing errors
CSCsr93911	GTP: Update PDP context request with 0x00000000 TEID is dropped
CSCsr94408	FWSM 3.2: np fast-path hangs while enqueueing in Syslog thread.
CSCsu02947	FWSM: Traceback in Thread Name fast_fixup
CSCsu43711	FWSM Reloads When Failover Peer is an ASA
CSCsu56194	Tcp state bypass feature is not working when a new vlan is configured
CSCsu56549	acl syslogs show hashvalue 0 for explicit ACE with modified log parametr
CSCsu60405	FWSM Replaces URL with IP Address for HTTP 1.0 URL Filtering Requests
CSCsu83857	console hung after "access-list commit" in 3.2.8 and 4.0
CSCsu85193	FWSM - policy nat rules are not replicated to standby
CSCsv00658	FWSM ACL optimization may result in corrupted ACLs
CSCsv08578	ICMP checksum not recalculated after modifying inner IP header checksum
CSCsv19445	FWSM may not program routes into NP3 upon bootup.
CSCsv21077	FWSM traceback in fast_fixup
CSCsv24161	FWSM3.2: Loss of connectivity when failover occurs in active/active mode
CSCsv24650	'show perform detail' does not show correctly udp statistics

**Table 13**      **Resolved Caveats in Release 4.0(4) (continued)**

<b>Caveat ID</b>	<b>Description</b>
CSCsv25111	FWSM trasnmits out of range traps to syslog server.
CSCsv49613	FWSM, TCP Checksum Error on certain packets
CSCsv50022	FWSM goes into a reboot loop when trying to convert http inspection map
CSCsv74061	fwsm 3.2.x - inspection - sunrpc-server cmd only works with /32 mask
CSCsv92418	FWSM crash Thread Name: doorbell_poll 0x5f2b NP2 thread
CSCsw79921	FWSM stops passing traffic when completion-unit enabled
CSCsx16884	FWSM - traceback with thread name np_cls_download_process
CSCsx18813	IP Fragmented Multicast packets not passed through FWSM for some groups

## Resolved Caveats in Software Release 4.0(3)

- CSCso25009

Performing a capture on the FWSM egress interface might show corrupted packets. This effect does not impact real traffic going through the FWSM.

**Workaround:** None.
- CSCsq17924

After the supervisor has an SSO switchover (where the secondary supervisor now becomes primary), if you reload the FWSM, then the FWSM will hang.

**Workaround:** To reset the FWSM, enter the **hw-module module module\_number reset** command at the switch CLI, or power cycle the FWSM in configuration mode by entering the **no power enable module module\_number** command, then the **power enable module module\_number** command.
- CSCsr56179

If you use a time range in an access list and use manual commit of access lists, access list optimization may not take place correctly even when the access list is active.

**Workaround:** Use auto-commit mode for access lists.
- CSCsr57503

When the access list is configured with the **interface** keyword, and the access list commit mode is manual, then if you change the interface IP address, the access list optimization will not happen correctly.

**Workaround:** Use auto-commit mode for access lists.

The caveats listed in [Table 14](#) were resolved in software Release 4.0(3), 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**      **Resolved Caveats in Release 4.0(3)**

<b>Caveat ID</b>	<b>Description</b>
CSCsf03695	Crash while creating captures for FWSM
CSCsi54863	FWSM: new MPC command to clear TCP Sack-Permitted option in 3WHS - SACK
CSCsk55964	FWSM reports WARNING: Restoring security context mode failed.
CSCso02252	Overlapping networks dont translate DNS address in 3.1.x
CSCso14430	“clear xlate state” not working
CSCso38805	Add SCCP v17 support to FWSM
CSCsq16078	Various Stateful Failover failures in FWSM 3.1.10
CSCsq66164	106101: Number of cached deny-flows for ACL log generated incorrectly
CSCsq71071	FWSM crash in Thread Name: doorbell_poll 0x5d05 NP2 thread
CSCsq79074	TCP MSS Not Adjusted in TCP SYN/ACK Segment
CSCsq87373	In Multicontext Mode Secondary FWSM crashes when committing configuration
CSCsq90172	NP-CP Bridge Block Deficiency with ICMP Activity To or From the Blade
CSCsr01682	OSPF losing neighbors during failover
CSCsr05764	FWSM blocks traffic due to route mismatch in CP and NP, NIC underruns
CSCsr06384	'aaa authen clear-conn' cannot be confgd after 'aaa authen include ip'
CSCsr11309	FWSM/TFW: rewrites MAC address for return traffic to HSRP address
CSCsr11384	url-filtering is not working for same-security traffic
CSCsr11888	Capture Output for Inspected Traffic Shows Corrupted
CSCsr11941	Display of access-list hash different between logs and access-list
CSCsr12059	FWSM NP Hard Debug: NP1 thread 19 hit PC 0x3cf5
CSCsr13642	New capture does not capture ingress packets after deleting old capture
CSCsr14332	FWSM may calculate ACL line numbers incorrectly in manual commit mode
CSCsr19679	Clear url-server stats is not clearing the Requests dropped counter
CSCsr21268	FWSM crashed at time_range.c after enabling failover
CSCsr24448	SIP Connection Dropped Abnormally on FWSM
CSCsr24521	Remark ACE get reordered when obj-grp ACE deleted in manual-mode
CSCsr24913	Outside nat does not use ACE added to policy ACL with line 1
CSCsr27446	Reordering of Remark ACE when grp-obj of obj-grp used by ACL is deleted
CSCsr29780	3.1.10.10: New ACE not getting added to correct line no. in manual mode
CSCsr36640	Failover inconsistency while shutting down and removing vlan's
CSCsr36669	Prevent overlapping names in config-url disk:
CSCsr36738	FWSM crashes in ci/console on deleting 'aaa authenticating include ip'

**Table 14** *Resolved Caveats in Release 4.0(3) (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCSr40940	FWSM snmp responses indicate flapping links
CSCSr40970	Strict HTTP inspection - problems with out-of-order packets from server
CSCSr42914	Overlapping address for nat and pat should show proper errors
CSCSr45802	FWSM fails over when compiling ACLs if CPU also busy inspecting traffic
CSCSr46459	Crash in Thread name dhcp_daemon related to DHCP relay
CSCSr47554	AAA Authentication request packet for 'show running-config' corrupted
CSCSr48265	3.2.7.3: http login does not reprompt on empty passwd if virtual telnet
CSCSr50360	Capture not working properly when same capture used for 2 interfaces
CSCSr55698	Capture not removed with 'no capture' when multiple cap. on same intf.
CSCSr60110	3.2.7.4: 'clear-conn' cannot be removed by 'no' statement
CSCSr60593	FWSM: May crash in Thread Name: accept/http
CSCSr62662	FWSM may crash during 'fsck disk:' operations
CSCSr67375	FWSM crashes in accept/http when deploying 'nat (0) 0 20.2.1.1' from CSM
CSCSr69909	snmp-map attached to inspect getting deleted with clear conf
CSCSr71168	Traceback: Crash in Thread Name: Route cache
CSCSr75501	FOVER:Standby MAC addr is improperly registered as Active MAC on Primary
CSCSr83441	Crash in manual mode (ACL optimization enabled) when deleting a rule
CSCSr83767	Clear route permanently removes static routes from the NP 3
CSCSr84424	Inter-context traffic on shared vlan fails starting in version 4.0
CSCSr93090	High CPU on FWSM due to AAA accounting/authentication
CSCSr93323	FWSM 4.0: Crash at ssh_receive
CSCSr93953	FWSM doesn't inspect the 3way hand shake for FTP data channel
CSCSr94374	DNS Responses Destined to Port UDP/53 are Blocked

## Resolved Caveats in Software Release 4.0(2)

- CSCsm69869

When an outside NAT rule is configured on the FWSM and NAT control is enabled, inbound traffic not matching that rule is being silently dropped.

**Workaround:** There are two options for getting around this. If possible, disable NAT control by entering the **no nat-control** command. If there are a limited number of networks on the outside coming in, a static outside NAT rule can be configured for those specific networks. For example:

```
static (outside,inside) 192.168.10.0 192.168.10.0 netmask 255.255.255.0
```

- CSCso22765

FWSM gives an error and discards the configuration when overlapping **static** commands are configured. For example:

```
static (inside,outside) tcp 192.168.1.100 www 192.168.2.100 www netmask
255.255.255.255
```

```
static (dmz,outside) 192.168.1.100 192.168.3.100 netmask 255.255.255.255
```

**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** command.

- CSCso46878

An extra xlate (between the wrong interfaces) gets created when using static policy NAT and the **no nat-control** command. This seems to occur when the policy NAT access list overlaps with a network on another interface.

**Workaround:** If applicable, use static NAT without an access list, and filter with an **access-group** command.

- CSCso92458

In multiple context mode, if you change the system configuration and a context configuration, and reload without first saving, then you are prompted to save the configurations; the configurations get saved even after typing **N** at the confirm prompt.

**Workaround:** None.

- CSCsq12999

When you configure TCP state bypass and match an access list in the class map that uses the **time-range** option, then a Telnet connection does not have TCP state bypass applied when the access list becomes active from an inactive state.

**Workaround:** In the class map, remove the **match access-list** command and add **match any**.

- CSCsq19931

A crash could occur if the following conditions are met:

- Access list group optimization is enabled
- An ACE is removed from the beginning of an access list, and a remark is added at the beginning of an access list both at the same time.

**Workaround:** Delete the ACE first and wait for optimization to complete then add the remark.

- CSCsq24440

In an Active/Active failover configuration, you cannot disable access list optimization in a context that is active on the secondary FWSM; the CLI prompt to disable optimization appears on the primary FWSM, and not the secondary.

**Workaround:** On the primary unit, do the following:

- Set group 2 to be active on the primary FWSM by entering the **failover active group 2** command.
- Disable optimization by entering the **no access-list optimization enable** command.
- Set group 2 to be active on the secondary FWSM again by entering the **no failover active group 2** command.

The caveats listed in [Table 15](#) were resolved in software Release 4.0(2), 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** *Resolved Caveats in Release 4.0(2)*

Caveat ID	Description
CSCsq71071	FWSM crash in Thread Name: doorbell_poll 0x5d05 NP2 thread

## Resolved Caveats in Software Release 4.0(1)

- CSCsm42519

Under rare circumstances when you configure AAA for network access using a RADIUS server, the FWSM might crash due to processing of authentication requests through the FWSM.

**Workaround:** None.

The caveats listed in [Table 16](#) were resolved in software Release 4.0(1), 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** *Resolved Caveats in Release 4.0(1)*

Caveat ID	Description
CSCsi27512	FTP with multiline 221 lines closes the connection too early
CSCsi73738	High CPU due to ACK storm with a TCP-based inspection enabled
CSCsk41644	FWSM - Issue with sending multiple GETs to the WebSense Server
CSCsk73347	NAT Bitmap Corruption Under High Xlate Use on FWSM
CSCsl04546	FWSM: Crash in Thread Name: websns_rcv_udp
CSCsl05878	FWSM reload with panic: route_process
CSCsl12104	Modifying fixup protocol icmp at a context affects other contexts (3.1)
CSCsm11988	Unable to clear uauth entry by username if username includes backslash
CSCsm35626	FWSM 3.2.2 - conns per sec usage under asdm not accurate
CSCsm41796	After failover, inspect ftp does not work - data channel not opened
CSCsm50370	ip address command breaks routing with duplicate statics
CSCsm58073	When saving a config to disk:/, the time is one day ahead
CSCsm60610	ACL:Cannot configure Access-list with udp port eq 0 on FWSM
CSCsm66984	FWSM resets intermittently
CSCsm68082	Error: Bad Octal (digit > 7) may appear with MGCP inspect
CSCsm69810	Outside NAT fails with outside NAT exemption
CSCsm84230	Policy Nat stops working when ACE duplicated through obj-grp and deleted
CSCsm86434	FWSM user auth dialogue box not re-presented for longer period in 3.1.8

**Table 16** *Resolved Caveats in Release 4.0(1) (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCsm87914	FWSM 3.2 crash in Thread Name: Logger
CSCso00289	Unable to Disable TCP Sequence Number Randomization
CSCso03094	Traceback in 'perfmon' thread
CSCso06060	Failover packet from FWSM has incorrect DSCP value
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.
CSCso40091	FWSM may delay URL Server checks causing a server to be marked DOWN
CSCso42729	Sunrpc sessions are not deleted from np 3 established list
CSCso59847	FWSM: Crash in thread skinny.
CSCso69586	FWSM failover pair with vlan mismatch may go active/active
CSCso92618	Inbound inspected tcp connections incorrectly timing out due to gc

## Related Documentation

See the following sections for related documentation:

- [Hardware Documents, page 35](#)
- [Software Documents, page 35](#)

## Hardware Documents

See the following related hardware documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation and Verification 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 using the CLI*
- *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 System Log Messages*

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide using ASDM*
- *Release Notes for Cisco ASDM*
- *Open Source Software Licenses for FWSM*
- *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, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2011 Cisco Systems, Inc. All rights reserved.