



Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 3.2(x)

September 2009

This document contains release information for the following FWSM releases:

- 3.2(15)
- 3.2(14)
- 3.2(13)
- 3.2(12)
- 3.2(11)
- 3.2(10)
- 3.2(9)
- 3.2(8)
- 3.2(7)
- 3.2(6)
- 3.2(5)
- 3.2(4)
- 3.2(3)
- 3.2(2)
- 3.2(1)

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](#)



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

© 2009 Cisco Systems, Inc. All rights reserved.

- [New Features, page 4](#)
- [Software License Information, page 7](#)
- [Limitations and Restrictions, page 7](#)
- [Open Caveats, page 9](#)
- [Resolved Caveats, page 12](#)
- [Related Documentation, page 33](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 34](#)

Important Notes

- You must install maintenance software Release 2.1(2) or later before you upgrade to FWSM Release 3.2. See the *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1* for detailed information about upgrading to 2.1(2).
- For traffic that passes through the control-plane path, such as packets that require Layer 7 inspection or management traffic, the FWSM sets the maximum number of out-of-order packets that can be queued for a TCP connection to 2 packets, which is not user-configurable. All 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, the System Execution Space Authentication feature in FWSM Release 3.2(1) 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, 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.

Upgrading or Downgrading the Software

See the *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1* for detailed information about upgrading to Release 3.2. Although the guide discusses upgrading to Release 3.1, the procedures also apply to upgrading to Release 3.2. You do not have to upgrade from 2.3 to 3.1 first, and then upgrade to 3.2; you can upgrade directly from 2.3 to 3.2.

Downgrading from a 3.2(x) image to a 3.1(x) image is supported when there are no 3.2(x) features configured. If the BGP stub license is activated, then downgrading to 3.1(1) through 3.1(7) will reset the activation key (3.1(8) and later is not affected). For example, if your activation key also includes a 50-context license, then resetting the key sets the license to the default 2 contexts.

Starting with Release 3.2(1), the vendor name in the **url-server** command changed from **n2h2** to **smartfilter**. Due to this change, if you downgrade a 3.2 or later image that has the **url-server vendor smartfilter** command to a 3.1 image, then the 3.1 image rejects the **url-server** command. You will have to re-enter the **url-server** command using the **n2h2** keyword.

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 3](#)

Catalyst 6500 Series Requirements

[Table 1](#) shows the supervisor engine version and software.

Table 1 **Support for FWSM 3.2 on the Catalyst 6500**

	Supervisor Engines ¹
Cisco IOS	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	22, 720, 32
Cisco IOS Software Modularity	
12.2(18)SXF4	720, 32

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 3.2 on the Cisco 7600**

	Supervisor Engines ¹
Cisco IOS	
12.2(33)SRA	720, 32
12.2(33)SRB	720, 32

Table 2 Support for FWSM 3.2 on the Cisco 7600

	Supervisor Engines ¹
12.2(33)SRC	720, 32, 720-1GE
12.2(33)SRD	720, 32, 720-1GE

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

Management Support

The FWSM supports the following management methods:

- Cisco ASDM—Software Release 5.2F supports FWSM software release 3.2(x) features. ASDM is a browser-based configuration tool that resides on the FWSM. The system administrator can configure multiple security contexts. If desired, individual context administrators can configure only their contexts.
- Command-line interface (CLI)—Access the CLI by sessioning from the switch or by connecting to the FWSM over the network using Telnet or SSH. The FWSM does not have its own external console port.

New Features

Table 3 lists the new features for Version 3.2(1).


Note

No new features were added in subsequent maintenance releases.

Table 3 New Features for FWSM Release 3.2(1)

Feature	Description
Routing	
BGP Stub Routing	The FWSM supports BGP stub routing. The BGP stub routing process advertises static and directly-connected routes but does not accept routes advertised by the BGP peer.
High Availability	
Failover Preemption for Active/Standby Failover	You can configure failover preemption for units in an Active/Standby failover configuration. When the primary unit in an Active/Standby failover configuration fails, or if the secondary unit boots before the primary unit, the secondary, standby unit becomes active. Configuring failover preemption causes the primary unit to automatically become the active unit after a specified amount of time.
AAA State Replication	FWSM synchronizes the user authentication table when Stateful Failover is enabled so the user does not have to authenticate once again after failover happens.
Application Inspection	

Table 3 **New Features for FWSM Release 3.2(1) (continued)**

Feature	Description
SIP Enhancement	SIP enhancements allow FWSM to clear media connections on receipt of a 200 OK for BYE message, on receipt of a 200 OK for CANCEL message, or on receipt of 200 OK for 4xx/5xx/6xx Error messages. Previously, media connections were cleared only due to an idle timeout. This enhancement also makes embryonic connections timeout no longer based on the configurable timeout sip-invite command or on the expiry field in the SIP invite message.
RTSP PAT	This release introduces PAT support in RTSP. For the RTSP PAT feature, if the translated port is different from the original port in an RTSP control channel message exchange, the translated port number is included in the RTSP packet before it is sent to the server. This ensures that the server responds on the correct port for the client.
H.323 GUP Support	The H.323 GUP support feature includes a separate inspection module that receives packets via dynamic inspection logic. This new inspection opens up pin-holes for establishing connection among Cisco gatekeepers working as clusters to provide gatekeeper redundancy to H.323 gateways.
MS-RPC (DCERPC) Inspection	Microsoft Remote Procedure Call (MSRPC) is a protocol used by the Microsoft distributed client and server applications. It is based on the DCERPC (Distributed Computing Environment Remote Procedure Call) protocol standard and has been modified and enhanced by Microsoft. It allows software clients to execute programs on a remote server. This involves client querying a server called the Endpoint Mapper (EPM) listening on a well known port number (TCP 135) for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. When FWSM is between a client and the EPM, the FWSM will allow the appropriate port number and network address through the firewall. It also applies NAT if needed for the secondary connection.
Interoperability with WAAS products	Wide Area Application Services (WAAS) products intercept connections and apply traffic optimization. With this feature, FWSM allows seamless integration with WAAS products.
GGSN Load Balancing	The GGSN load balancing feature allows any GNS belonging to a GNS pool to respond to an SGSN request to achieve load balancing on the GGSNs. The inspection engine allows a set of GNS to respond to a request even if a GSN is not specified as the responder to the request in the GTP request message.
Transparent Firewall	
Transparent Firewall NAT Support	<p>You can now configure NAT for a transparent firewall. This feature extends the NAT/PAT functionality to transparent mode thereby reducing the need for adding a new NAT/PAT device in the network. This feature is also very useful in cases where multiple virtual routing and forwarding (VRFs) with overlapping addresses are used. NAT per VRF is not supported on the Catalyst 6500 series switches and the Cisco 7600 series routers.</p> <p>Introducing NAT support for transparent firewalls addresses the NAT per VRF requirement. Transparent mode offers the capability to run routing protocols through the FWSM with minimal configuration.</p>
NAT	
NAT Bypass No Longer Creates NAT Sessions	In previous releases, even if you used NAT exemption or identity NAT, the FWSM created NAT sessions (xlates) for all flows. In Release 3.2, you can configure the FWSM to create xlates only when NAT is configured. By default, the FWSM creates NAT sessions for all connections even if you do not use NAT. For example, a session is created for each untranslated connection even if you do not enable NAT control, you use NAT exemption or identity NAT, or you use same security interfaces and do not configure NAT. Because there is a maximum number of NAT sessions, these kinds of NAT sessions might cause you to run into the limit. To avoid running into the limit, you can disable NAT sessions for untranslated traffic using the xlate-bypass command.

Table 3 ***New Features for FWSM Release 3.2(1) (continued)***

Feature	Description
AAA	
Authentication Support When Sessioning To The System Execution Space	When you log in to the system execution space from the switch in multiple context mode, a new feature 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, 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.
Direct Login Or Logout Using Virtual HTTP and SSH For User Authentication	In addition to direct login with virtual Telnet, you can now log in or out directly using HTTP and SSH.
Virtual HTTP Hostname Support	You can now assign a hostname to the virtual HTTP server on the FWSM. When a user is forwarded to the virtual HTTP server to enter their AAA username and password, you see the hostname in the authentication dialog box message. This information helps differentiate the AAA prompt from the destination HTTP server prompt.
Interactive Password Prompts With RADIUS For Authentication	With RADIUS servers, a user can now be prompted for a new password when authenticating.
Command authorization enhancement	This feature makes FWSM command string handling consistent with Cisco IOS software.
Cut through proxy enhancement	FWSM tears down all connections when the uauth timer expires.
TCP	
TCP State Bypass	If you have asymmetric routing configured on upstream routers, and traffic alternates between two FWSMs, then you can configure TCP state bypass for specific traffic.
Connection Timeouts For Non-TCP Traffic On A Per-flow Basis	You can now configure connection timeouts for non-TCP traffic using Modular Policy Framework. Formerly, you could only set global timeouts.
Switch Integration	
IOS Support For Autostate Messaging For Rapid Link Failure Detection	Using Catalyst operating system software Release 8.4(1) and higher or Cisco IOS software Release 12.2(18)SXF5 and higher, the supervisor engine can send autostate messages to the FWSM about the status of physical interfaces associated with FWSM VLANs.
Miscellaneous	
SNMP Enhancement	SNMP CLI, MIB and trap enhancements have been added in Release 3.2(1).
DHCP Relay per interface	An option is provided to the user to configure DHCP helper addresses on a per-interface basis.

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

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.
- 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.
- For ICMP traffic to pass through the FWSM when the don't fragment (DF) bit is set, be sure to enable ICMP application inspection. When ICMP inspection is disabled, the FWSM NATs the packet and then checks the MTU. If the MTU is exceeded and the DF bit is enabled, the FWSM should send an ICMP unreachable packet back to the sender. But because the packet was already NATted, the FWSM no longer has the source IP address, so it drops the packet. (CSCsk61721)

- If you configure the **set connection timeout tcp** and **set connection timeout idle** commands for the same class, then the **idle** command (which sets the timeout for all types of connections) is used instead of the **tcp** command (which sets the timeout for TCP connections only) when the class map does not specifically match TCP traffic. If the class map matches an access list that specifies TCP traffic explicitly, then the **tcp** command is used instead of the **idle** command for TCP traffic; other traffic that matches the access list uses the **idle** command. The following example creates an access list with an ACE that specifically matches TCP traffic. Therefore, TCP traffic uses the **tcp** command, while UDP and ICMP traffic uses the **idle** command.

```
access-list ip_traffic extended permit tcp any any
access-list ip_traffic extended permit udp any any
access-list ip_traffic extended permit icmp any any

class-map c1
  match access-list ip_traffic

policy-map p1
  class c1
    set connection timeout idle 3:0:0
    set connection timeout tcp 2:0:0

service-policy p1 global
```

The following example has an access list that matches all IP traffic, and it does not specifically match TCP traffic. Therefore, even though the **tcp** command is present in the configuration, it is ignored in favor of the **idle** command for all traffic, including TCP traffic.

```
access-list ip_traffic extended permit ip any any

class-map c1
  match access-list ip_traffic

policy-map p1
  class c1
    set connection timeout idle 3:0:0
    set connection timeout tcp 2:0:0

service-policy p1 global
```

(CSCsk57385)

- The FWSM processes virtual Telnet connections after you remove the **virtual telnet** command. You need to reload the FWSM after you remove the **virtual telnet** command to avoid the following situation.

After you remove the **virtual telnet** command, the FWSM processes virtual Telnet connections as through the box connections and thinks there is a host on the inside with the virtual IP address. Because AAA is configured for through the box connections, a uauth is created. Once a uauth is created, the connection is forwarded to the specific IP address. Because no hosts are available at this IP address, the connection is closed. However, the uauth remains and all connections through the box go through until the uauth times out. You cannot clear a uauth if the FWSM sees an invalid host. It needs to be done via an access-list to check the connections going through the box. (CSCsl08082)
- 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)

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 3.2(4), then you need to add the caveats in this section to the resolved caveats from 3.2(5) and later to determine the complete list of open caveats.

- CSCei76209
The **show mroute output** is missing interfaces in the OIF list after it switches to the shortest path tree (s,g). The **show mfib** output shows this correctly.
Workaround: None.
- CSCsi03512
You cannot ping across the FWSM after entering the **[no] fabric sw-mode force bus** command on the switch. This happens when switching mode is toggled on a Catalyst 6500 with supervisor 720 from Truncated mode to Bus mode and back to Truncated mode.
Workaround: Reload the Catalyst 6500 switch.
- CSCsj04940
When configuring the **nameif** command in single transparent mode, portmap_index: unable to locate fixup message. Message is seen only in Transparent mode.
Workaround: None.
- CSCsj98260
Under extreme traffic conditions, the FWSM crashes with continuous GTP V1 PDP context creation and delete requests.
Workaround: None.
- CSCsk06328
When you configure the **virtual http host warning** command, the FWSM displays the wrong URL on the client browser.
Workaround: None.
- CSCsk82919
If you use more than 70 dynamic access lists for a single user, the 71st dynamic access list or beyond may not load in the access list, and unpredictable behavior may occur; for example, you might not be able to FTP to the server.
Workaround: Limit dynamic access lists to 70 or below per user.
- 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 through registration should be allowed. For example, the **pim rp-address** command is used in conjunction with an access list similar to 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.

- 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**.

- CSCsq11637

In transparent mode, when a user initiates an inbound Telnet connection, the user is prompted for the AAA username and password. After the user enters the correct AAA username and password, the Telnet sever login and password should be prompted. But is not prompted and the session times out. After the connection times out, the uauth session is still in the table. If you try to Telnet again, the connection succeeds. So, only the Telnet used to create the uauth session fails. This issue is seen when the configuration has the following:

- Transparent mode AAA authentication on the outside interface for inbound traffic from outside to inside.
- A static NAT statement present of the form **static (inside,outside)** (notice it should be **(inside,outside)** not **(outside,inside)**).
- The static NAT statement is *not* identity static NAT (where the real and mapped IP address of the inside host are the same).

Workaround: Avoid non-identity static NAT of the form **static (inside,outside) A B** on the inside interface. If the **nat-control** command is enabled, either configure identity static NAT or NAT exemption on the inside interface. Or simply reconnect with Telnet after the uauth session is created.

- CSCsv50778

If you configure policy NAT using an access list that is inactive, and then change the memory partition of the context using the **allocate acl-partition** command, then the traffic starts using the policy NAT having an inactive access list to create xlates. You can also see that the hitcnt of the access lists start incrementing when it is still in an inactive state.

Workaround: Reload the FWSM.

- CSCsw36835

When you share an outside interface among multiple contexts, and a host in context 1 connects to a host in context 2 using UDP, then if you clear the connection in one of the contexts (for example, using **clear local-host** or **clear xlate**), then any subsequent UDP connections between the two hosts fail.

Workaround: Clear the connection in both contexts.

- CSCsw51353

When you change the memory partition of a context, then all access lists that have the **log** keyword specified stop generating logs.

Workaround: Delete and reconfigure the access lists with the **log** keyword.

- CSCsw83232

Communication between H.323 endpoints might fail after a short amount of time (around 30 seconds) or might fail to be established at all. Note: 3.2(1) is not affected.

Workaround: Disable TCp normalization using the **no control-point tcp-normalizer** command.

- CSCsx79204

When PPTP connections are passed through the FWSM, if the PPTP inspection is enabled on the FWSM, then two GRE connections will be dynamically built by the inspection engine. These GRE connections will timeout after 2 minutes of inactivity even if the configuration on the FWSM specifies they should not time out at 2 minutes.

The following example enables PPTP inspection and an idle timeout of 24 hours:

```
access-list pptp extended permit gre any any
class-map pptp
  match access-list pptp
policy-map global_policy
  class-map pptp
    set connection timeout idle 24:00:00
```

Workaround: Disable the PPTP inspection, and explicitly allow the GRE traffic through the FWSM. If NAT is used, the inside hosts using PPTP must be statically NATted through the FWSM.

- CSCsy17449

Entering the **write net** command within a context unexpectedly reloads the FWSM; you see the following:

```
NP Hard Debug: NP1 thread 15 hit PC 0x597f
LCBA
```

Workaround: None.

- CSCsy74687

You might experience an unexpected reload in Thread Name: doorbell_poll or Syslog_entry.

Workaround: None.

- CSCsz82463

FWSM is not correctly parsing the RTSP setup messages and opens a connection stream on the wrong port.

Workaround: None.

- CSCsz74961

FWSM is logging incorrect system messages for DNS traffic which are then denied in an ACL. This occurs only when DNS is enabled.

Workaround: None.

- CSCsz81503

Multicast bi-directional forwarding fails due to an incorrect forwarding entry. The results can be seen when you use 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 routing protocol.

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

- CSCta28599

In certain instances when setting up failover, FWSM may crash and reload due to a problem with Thread Name: fover_health_monitoring_thread entry.

Workaround: None.

Resolved Caveats

This section contains resolved caveats in each maintenance release, and includes the following topics:

- [Resolved Caveats in Software Release 3.2\(15\), page 12](#)
- [Resolved Caveats in Software Release 3.2\(14\), page 13](#)
- [Resolved Caveats in Software Release 3.2\(13\), page 14](#)
- [Resolved Caveats in Software Release 3.2\(12\), page 15](#)
- [Resolved Caveats in Software Release 3.2\(11\), page 16](#)
- [Resolved Caveats in Software Release 3.2\(10\), page 18](#)
- [Resolved Caveats in Software Release 3.2\(9\), page 19](#)
- [Resolved Caveats in Software Release 3.2\(8\), page 21](#)
- [Resolved Caveats in Software Release 3.2\(7\), page 23](#)
- [Resolved Caveats in Software Release 3.2\(6\), page 24](#)
- [Resolved Caveats in Software Release 3.2\(5\), page 26](#)
- [Resolved Caveats in Software Release 3.2\(4\), page 29](#)
- [Resolved Caveats in Software Release 3.2\(3\), page 30](#)
- [Resolved Caveats in Software Release 3.2\(2\), page 32](#)

Resolved Caveats in Software Release 3.2(15)

This section contains resolved caveats in software Release 3.2(15).

- CSCtc02363

The RTSP inspection incorrectly translates IP addresses inside the URL in RTSP OPTIONS and DESCRIBE headers.

Workaround: None.

- CSCtb88893

In transparent mode when using failover, the broadcast ARP request from the standby unit is being passed through by the active FWSM. This causes a MAC address change on the switch, and as a result, keepalives between the FWSMs are failing. You might see the following syslog messages:

FWSM-1-105005: (Primary) Lost Failover communications with mate on interface trusted2030

FWSM-1-105008: (Primary) Testing Interface trusted100

FWSM-1-105009: (Primary) Testing on interface trusted100 Passed

Also, traces indicate that hellos are being missed between the active and standby FWSM.

Workaround: None.

- CSCtb18847

When using the **established** command, all traffic stops passing through the FWSM, and failover does not occur. When viewing the output of the **show np pc** command at separate times, note that the threads in the third column (NP3) will not change.

Workaround: Remove the **established** commands.

The caveats listed in [Table 4](#) were resolved in software Release 3.2(15), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 4 **Resolved Caveats in Release 3.2(15)**

Caveat ID	Description
CSCsz35702	Portmap translation error after forcing switchover
CSCta64836	Firewall blade unexpectedly 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
CSCtb49822	http traffic with segmented GET blocked by url-filtering configuration
CSCtb76719	Meaning of Flags 's' and 'S' is Reversed in 'show conn detail' Output
CSCtc36009	TCP reset option incorrectly appears in set connection timeout command
CSCtc36050	capture feature shows ICMP payload modified by firewall when it is not
CSCtc36380	FWSM corrupts ICMP checksum in ICMP unreachable packets
CSCtc36651	FTP fails in Active/Active mode when two contexts not active on same FW
CSCtc40207	Standby transparent FWSM might send arp request using active MAC
CSCtc68193	snmp query for any OID under 1.3.6.1.2.1. causes np xlate query
CSCtc71533	IPv6 object-group does not allow group-objects
CSCtd04061	IMPORTANT TLS/SSL SECURITY UPDATE

Resolved Caveats in Software Release 3.2(14)

This section contains resolved caveats in software Release 3.2(14).

- CSCta49185

When FWSM is in multi-context mode and the **wr standby** command is run in user context mode on Active unit, the configuration is not the same as the configuration on the standby unit.

Additionally, the **snmp-server enable traps snmp authentication linkup linkdown coldstart** configuration appears on both the Active and Standby units.

Workaround: None.

The caveats listed in [Table 5](#) were resolved in software Release 3.2(14), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 5 Resolved Caveats in Release 3.2(14)

Caveat ID	Description
CSCsz92926	FWSM OSPF process stops sending out LSA with large amount of link IDs
CSCta06559	Inspect SIP shows error "portmap_index: unable to locate fixup"
CSCta08654	Interface in shut down status intercepts traversing traffic
CSCta44620	Software Forced reset in fast_fixup with multiple FTP connections
CSCta44761	FWSM - SIP inspection treats User-agent Version number as IP address
CSCta47271	Software forced reset after enabling 'debug sunrpc'
CSCta58464	FTP data connection times out
CSCta58702	FWSM pause indefinitely due to high icmp traffic through 2 mgt sessions
CSCta60764	Cut-thru-proxy:certificate error after completion of initial authenticati
CSCta64995	# (hash) is lost from per-host snmp-server community after bulk sync
CSCta68828	FWSM forming OSPF adjacency with 5 seconds delay
CSCta73803	concurrent snmpwalk across many contexts causes loss of 16384 blocks
CSCta83188	Syslog 111008 doesn't display the subnet mask with the network-object cm
CSCtb03565	FWSM corrupts ICMP time to live exceeded with MPLS TAG
CSCtb23513	Authentication in progress sessions not removed with DACLs
CSCtb29859	NP hang where NP 3 fails to communicate with NP1/2
CSCtb34170	Static PAT causing failure for traffic from inside

Resolved Caveats in Software Release 3.2(13)

This section contains resolved caveats in software Release 3.2(13).

- CSCsy35054

When receiving a gratuitous ARP, the FWSM may not update all existing connections with the new MAC address.

Workaround: Enter the **clear local-host** command for the affected host to clear out the old MAC address; the client must re-establish any connections to that host.
- 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.
- CSCsz23283

When snmpwalk is issued to the FWSM, the FWSM may respond TCP-MIB in non-lexicographical order.

Workaround: Run snmpwalk with the -Cc option.
- CSCsz60413

The FWSM unexpectedly reloads when you enter the **show failover history** command when the FWSM has frequent failover state changes.

Workaround: Do not enter the **show failover history** command in the above circumstances.

The caveats listed in [Table 6](#) were resolved in software Release 3.2(13), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 6 *Resolved Caveats in Release 3.2(13)*

Caveat ID	Description
CSCsv22070	Logging to the console causes syslogs to be rate-limited
CSCsx97979	ENH show np x thread - should display all thread output.
CSCsy01150	Show service-policy flow tcp command is broken.
CSCsy88893	Should warn about impossible next hop of static route.
CSCsz22099	XLATE on shared interface causes bad connection with high data rate.
CSCsz47735	FWSM doesn't support H323 with VCON MXM 4.7 and XPoint 7.500.062.
CSCsz49945	Copy flash:startup-config tftp traffic passing through the user context.
CSCsz57041	Inconsistent behavior in adding access-list remark in manual-commit mode
CSCsz51960	Traceback with Thread Name: fover_ifc_test on standby module.
CSCsz66958	FWSM should send gratuitous ARP if new Primary inserted in failover.
CSCsz68425	Transparent FWSM not Sync'ing Valid CAM Table Entries to Failover Peer.
CSCsz73675	FWSM crash in ssh thread during dhcrelay config.
CSCsz75402	TCP checksum errors after failover for new connections.
CSCsz79758	H323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT.
CSCsz97207	NP 2 threads lock due to processing malformed IP packet.
CSCta13098	FWSM sends TCP RST with wrong ACK nbr.
CSCta17569	Local-host objects not being freed.

Resolved Caveats in Software Release 3.2(12)

This section contains resolved caveats in software Release 3.2(12).

- CSCsy29192—**This caveat is open in Release 3.2.11 and later. This issue does not affect earlier releases.**

When using failover, HTTP connections are not being replicated properly to the standby unit. The connections are being replicated in a half-open state.

Workaround: None.

- CSCsr68825

When using failover, the standby FWSM may send the RST for some TCP connections. This is a rare situation that may occur either during the manual switchover, or during the transient conditions (the preemption is taking place, and so on).

Workaround: None.

- CSCsy00911
If you enable SMTP logging using the **logging mail** command, the amount of free memory on the FWSM gradually decreases with no changes in traffic load.
Workaround: Disable SMTP logging or reload the FWSM periodically.
- CSCsy03439
The FWSM in failover scenario does not send the coldstart SNMP trap.
Workaround: None.

The caveats listed in [Table 7](#) were resolved in software Release 3.2(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 7 *Resolved Caveats in Release 3.2(12)*

Caveat ID	Description
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
CSCsv82747	Bitmap corruption after switchover
CSCsx46210	RTCP connection torn down while the call is in progress
CSCsx54892	Non-standard log message format %FWSM--1-710002
CSCsx59229	Standalone 'Failover' Command Stops All Local Outgoing Traffic
CSCsx64037	ftp-bufferwrap stops functioning after few days
CSCsx66450	index value is incorrect when individually run snmpget for each ifindex
CSCsx67475	CPU problems and unexpected reload when large number of routes added
CSCsx75701	FWSM log 106101 triggered but max flows not reached
CSCsy06702	FWSM - virtual http x.x.x.x may disappear from the config after a reboot
CSCsy26815	Transparent FWSM treats incorrectly fragmented inspected h.323 packet
CSCsy34261	FWSM: 256 blocks get depleted by syslog messages
CSCsy34495	Incomplete dhcprelay config makes a valid one fail
CSCsy69895	Traceback in thread: sip
CSCsy95843	FWSM Traceback in fast_fixup
CSCsy97933	NAT exemption and dynamic NAT conflict between same-security interfaces

Resolved Caveats in Software Release 3.2(11)

This section contains resolved caveats in software Release 3.2(11).

- CSCsv14944
Crash in Thread Name: doorbell_poll, 0x3cec in NP1 or NP2.
Workaround: None.

- CSCsv42245
HTTP traffic fails for ASR topology with Active/Active failover.
Workaround: None.
- CSCsv99839
H.323 inspection fails to open pinholes for voice or video traffic of VCON MXM management software Version 4.7 used with VCON Version 8.0 clients.
Workaround: Downgrade the VCON MXM manager to 4.51 and the clients to 7.x.
- CSCsw40164
When failover interfaces are configured before any other VLAN interface, then for SNMP, the failover interfaces are included in ipAddrtable .1.3.6.1.2.1.2.2.1.2, but not in .1.3.6.1.2.1.4.20.1.2. This causes the indices for these two subtrees to be off by the number of failover interfaces configured.
Workaround: Remove the failover configuration and re-add it each time you add a new VLAN interface. This will cause the indices for the failover interfaces to be last and will not influence the index of any other interface.
- CSCsw46905
If you use Active/Active failover, during configuration replication, the active firewall might crash and hang.
Workaround: Reload the active FWSM from the switch is needed using the **hw-module module slot reset** command.
- CSCsv31759
When you enable ICMP inspection for an interface, it automatically gets enabled for the global policy.
Workaround: Manually disable ICMP inspection for the global policy.
- CSCsv84314
The FWSM may crash in Thread Name: doorbell_poll.
Workaround: None.

The caveats listed in [Table 8](#) were resolved in software Release 3.2(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 8 Resolved Caveats in Release 3.2(11)

Caveat ID	Description
CSCsl63063	FWSM - Crash in thread doorbell_poll: NP2 / PC 0x3a1a
CSCsr99226	Static PAT w/ACL on FWSM silently drops unmatched traffic
CSCsu21962	Crash in Thread Name: doorbell_poll
CSCsu26449	FWSM: Smart Filter URL filtering may break - FWSM may send reset
CSCsu46215	H.323 communication fails through FWSM with tcp-normalizer enabled
CSCsv46585	Modifying an ACL can cause traffic to be incorrectly allowed
CSCsw77676	FWSM: No logging message 710003 does not work

Table 8 *Resolved Caveats in Release 3.2(11) (continued)*

Caveat ID	Description
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
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
CSCsx82996	Traceback: doorbell_name

Resolved Caveats in Software Release 3.2(10)

This section contains resolved caveats in software Release 3.2(10).

- CSCsv41010
When SIP inspection is enabled, the FWSM crashes at thread name udp_sip.
Workaround: Disable SIP inspection.
- CSCsv54515
For connections like FTP, the data channel SYN is not adjusted if the **sysopt connection tcp window-scale** and **tcp-sack** options are configured.
Workaround: None.

The caveats listed in [Table 9](#) were resolved in software Release 3.2(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 9 *Resolved Caveats in Release 3.2(10)*

Caveat ID	Description
CSCeh90462	FWSM silently drops TCP SYN while cleaning up old connection
CSCsi30615	show version output shows: Int: Not licensed
CSCsk05321	'show connection detail' should show true interface names
CSCsl16482	HTTP authentication with ssl trust-point is not working after reload
CSCsv25111	FWSM transmits out of range traps to syslog server.
CSCsv49613	FWSM, TCP Checksum Error on certain packets
CSCsv73391	fwsn might drop multicast traffic with a static default mroute
CSCsv74061	fwsn 3.2.x - inspection - sunrpc-server cmd only works with /32 mask
CSCsv83322	FWSM 'Who' Command is Locked in Configuration Mode
CSCsv91984	Remove Warning message when enabling sysopt np completion-uni
CSCsw17796	FWSM access-group is not automatically updated for an ipv6 access-list

Resolved Caveats in Software Release 3.2(9)

This section contains resolved caveats in software Release 3.2(9).

- CSCsr11396

URL filtering stop when the **url-server** command is configured on either an inside or DMZ interface and application inspection is enabled in an interface-specific service policy.

Workaround: Enable application inspection in the global service policy.

All traffic fails through the context after changing the acl-partition of the context.

- CSCsr55215

The **auth-prompt reject invalid-credentials** command does not work. If a user gives the wrong username and password, the prompt is not displayed.

Workaround: Configure the reject prompt using the **auth-prompt reject prompt** command instead.

- CSCsr91871

When you have an SGSN context request/response inspected by the FWSM with a size above 32 bytes and a “next extension header type” of 0x00, then you see the following syslog message:

```
GTPv1 packet parsing error from inside:10.1.2.3/2123 to outside:10.2.2.3/2123, TEID: 0x00000000, Reason:
```

Workaround: Use the **permit error** parameter for the GTP inspection so that these packets are not dropped.

- CSCsr93090

When there is a heavy load of accounting and authentications being performed, you might see a high CPU condition.

Workaround: The issue is slightly improved if you add the AAA round-robin scheduling feature to the FWSM.

- CSCsr93879

GTP identification request/response packets are dropped by the FWSM, which generates the following syslog message:

```
%FWSM-3-324001: GTPv1 packet parsing error from inside:10.2.3.4/2123 to outside:10.3.4.5/2123, TEID: 0x00000000, Reason:
```

Workaround: Use the **permit error** parameter for the GTP inspection so that these packets are not dropped.

- CSCsr93911

When you configure the FWSM to inspect GTP traffic in a context where you switch from GTPv0 and GTPv1, then an update PDP context request with TEID = 0x00000000 will be dropped by the FWSM with the following syslog message:

```
%FWSM-3-324001: GTPv1 packet parsing error from inside:10.2.3.4/2123 to outside:10.3.4.5/2123, TEID: 0x00000000, Reason:
```

Workaround: Use the **permit error** parameter for the GTP inspection so that these packets are not dropped.

- CSCsr93953

When you enable FTP inspection, the packets on the data channel do not pass through the FWSM after the 3-way hand shake was done correctly. This can occur when the MTU on the involved interfaces is lower than the default (1500); also, when IP packets are sent on the FTP data channel that are bigger than the MTU of one of the involved interfaces.

Workaround: Increase the MTU of the interfaces up to the limit (1500). Have the client and the server configure the size of IP packets to be lower than the lowest MTU of the interfaces.

- CSCsr94408

The FWSM stops forwarding traffic due to a NP (Network Processor) being stuck. If you use failover, both units will report to be active. In the output of the **show tech** command or the **show np 1/2 stats** command, the following message can be seen:

```
ERROR: np_logger_query request for FP Stats failed
```

The **show np block** output will show thresholds hit massively and the **show np pc** output will show threads stuck on network processors.

See the following sample output from the **show np pc** and **show np block** commands:

```
hostname# show np pc
THREAD: PC (NP1/NP2/NP3)
 0:0000/6f4f/0000  1:0000/6f4f/0000  2:0000/6522/0000  3:0000/6522/0000
 4:0000/6f4f/0000  5:0000/40da/0000  6:0000/3e99/0000  7:0000/6c1c/0000
 8:0000/6f4f/0000  9:0000/6f4f/0000 10:0000/40da/0000 11:0000/40da/0000
12:0000/6f4f/0000 13:0000/40da/0000 14:0000/6f4f/0000 15:0000/40d8/0000
16:0000/6f4f/0000 17:0000/6522/0000 18:0000/40da/0000 19:0000/6f4f/0000
20:0000/3e99/0000 21:0000/3e99/0000 22:0000/3e99/0000 23:0000/6f4f/0000
24:0000/6f4f/0000 25:0000/4a84/0000 26:0000/40da/0000 27:0000/6f4f/0000
28:0000/3e99/0000 29:0000/6f4d/0000 30:0000/6f4f/0000 31:0000/6f4d/0000
```

```
hostname# show np block
          MAX   FREE  THRESH_0  THRESH_1  THRESH_2
NP1 (ingress) 32768   112    298078   2107651   33106766
   (egress)  521206 521206         0         0         0
NP2 (ingress) 32768   112    3467122   1266051   12020896
   (egress)  521206 113554         0         0         0
NP3 (ingress) 32768  32768         0    446820    1702936
   (egress)  521206 521206         0         0         0
```

Workaround: Regularly verify the **show np block** output to see if thresholds are not hit. If they are hit, consider routing some traffic outside of the FWSM.

- CSCsu03780

When you clear the uauth session using the **clear uauth** command, or after the uauth timer expires, all existing connections using the uauth get teared down. This problem occurs if the uauth was created using the **aaa authentication include ip** command.

Workaround: Avoid using the **aaa authentication include** command; use the **aaa authentication match** command instead. For example:

```
access-list aaa permit ip source dest
aaa authentication match aaa interface server
```

- CSCsu04081

The **aaa accounting include** command does not accept udp as one of the options.

Workaround: Use the **aaa accounting match** command instead.

The caveats listed in [Table 10](#) were resolved in software Release 3.2(9), and were not previously documented. If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 10 **Resolved Caveats in Release 3.2(9)**

Caveat ID	Description
CSCsf03695	Crash while creating captures for FWSM
CSCsm90200	FWSM show memory displays incorrect data in multi context mode
CSCsr73708	FWSM/NP3 all threads stuck at address 0x3300
CSCsr83767	Clear route permanently removes static routes from the NP 3
CSCsr85418	set connection timeout idle not working when it's set 1hr.
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 parameter
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
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

Resolved Caveats in Software Release 3.2(8)

This section contains resolved caveats in software Release 3.2(8).

- 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.

- CSCsq84306

SQL*net inspection modifies the HOST field of the redirect packet. The original content is replaced by the source IP address of the packet.

Workaround: Disable SQL*net inspection.

- CSCsq45659

For IPsec flows (ESP), the destination MAC address might be rewritten with the MAC address of the old gateway after the packet is processed by the FWSM. This only affects FWSM in transparent mode after a route change on adjacent routers/MSFC.

Workaround: Clear connections for affected hosts using the **clear conn local** *ip_address* command or the **clear conn global** *ip_address* command.

- CSCsq66164
Syslog message 106101 (number of cached deny flows) is generated constantly even though the number of deny flows has not reached the limit. This occurs when you have different time intervals set on ACEs.
Workaround: None
- CSCsq11512
A Telnet connection is not affected by the TCP state bypass feature when a class map access list with a time range goes from active to inactive.
Workaround: In the class map, remove the **match access-list** command and use **match any** instead or, if the **match access-list** command is required, disable the **set connection advanced-options tcp-state-bypass** command and re-configure it again after the access list becomes active.
- CSCsr11102
If the access list commit mode is set to manual-commit when you change the memory partition to which a context is assigned (the **acl-partition** command), then all subsequent traffic which was permitted and passing earlier now gets denied; syslog message 106023 is sent.
Workaround: Make sure the commit mode is set to auto-commit (the **access-list mode auto-commit** command) before changing the **acl-partition** command for a context.
If the issue has already appeared, then either change the mode to auto-commit and again change the **acl-partition** command; or clear the complete configuration of the context by entering the **clear configure all** command inside the context.
- CSCsr11384
URL filtering stops for same-security level traffic when the **url-server** command is configured on either an inside or DMZ interface and application inspection is enabled either globally or on an interface.
Workaround: Disable application inspection.

The caveats listed in Table 11 were resolved in software Release 3.2(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 11 Resolved Caveats in Release 3.2(8)

Caveat ID	Description
CSCsi54863	FWSM: new MPC command to clear TCP Sack-Permitted option in 3WHS - SACK
CSCsj17253	Log messages reported to console do not match message reported to HTTP
CSCsk55964	FWSM reports WARNING: Restoring security context mode failed
CSCso02252	Overlapping networks don't translate DNS address in 3.1.x
CSCsq16078	Various Stateful Failover failures in FWSM 3.1.10
CSCsq55205	MPF TCP timeout feature can not work with ACL deny entry
CSCsq61452	Multicontext FWSM pair has continual reload with no crashinfo written
CSCsq79074	TCP MSS Not Adjusted in TCP SYN/ACK Segment
CSCsq84306	SQLnet inspection overwrites HOST field in the redirect packet
CSCsq87373	In Multicontext Mode Secondary FWSM crashes when committing configuration

Table 11 *Resolved Caveats in Release 3.2(8) (continued)*

Caveat ID	Description
CSCsr01682	OSPF losing neighbors during failover
CSCsr05764	FWSM blocks traffic due to route mismatch in CP and NP, NIC underruns
CSCsr11309	FWSM/TFW: rewrites MAC address for return traffic to HSRP address
CSCsr11941	Display of access-list hash different between logs and access-list
CSCsr14332	FWSM may calculate ACL line numbers incorrectly in manual commit mode
CSCsr24448	SIP Connection Dropped Abnormally on FWSM
CSCsr29124	PAT src port allocation policy negates effect of host port alloc. policy
CSCsr40940	FWSM snmp responses indicate flapping links
CSCsr40970	Strict HTTP inspection - problems with out-of-order packets from server
CSCsr46459	Crash in Thread name dhcp_daemon related to DHCP relay
CSCsr47554	AAA Authentication request packet for 'show running-config' corrupted
CSCsr51684	ERROR: np_logger_query request.Traffic failing on FWSM
CSCsr60593	FWSM: May crash in Thread Name: accept/http
CSCsr62662	FWSM may crash during 'fsck disk:' operations
CSCsr75501	FOVER:Standby MAC addr is improperly registered as Active MAC on Primary
CSCsu01813	FWSM 3.2: redirected sqlnet data connections should not be inspected

Resolved Caveats in Software Release 3.2(7)

This section contains resolved caveats in software Release 3.2(7).

- 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
```

- CSCso10574

The FWSM might crash after upgrading to 3.2(4) or later, when multicast routing is enabled.

Workaround: Disable multicast routing before upgrading.

- 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.

The caveats listed in [Table 12](#) were resolved in software Release 3.2(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 12 **Resolved Caveats in Release 3.2(7)**

Caveat ID	Description
CSCsk98142	FWSM - Crash in thread doorbell_poll: NP1 or NP2 / PC 0x59c2 or 0x599b
CSCsl76198	FWSM: TCP State Bypass does not work on global policy
CSCsm09418	Standby FWSM forwards traffic
CSCso63107	"Unable to add, fixup config limit reached" when class-map has match ACL
CSCso65731	"write mem" from HTTPS adds no monitor-interface CLIs to startup config
CSCso65918	DNS guard does not close DNS connections in cascaded contexts
CSCso73260	FWSM sends ARP from shutdown interface during unit health monitoring
CSCso75761	portmap_index: unable to locate fixup appears when ACL is modified
CSCso95053	FWSM may report syslogs with very high port numbers
CSCsq09303	FWSM 3.1: allocate-acl-partition command makes inactive ACE active.
CSCsq09883	AAA shell command set fails for some commands
CSCsq19327	FWSM drops ftp "Response:125" after transferring 1900+ files
CSCsq27152	ASDM location commands do not appear in show run all output
CSCsq34233	FWSM: Enable check to disallow admin context in failover grp 2
CSCsq43713	With FWSM code 3.2(5) one of the FWSM goes in failed state
CSCsq55738	Addresses used in Static NAT are no longer advertised in OSPF

Resolved Caveats in Software Release 3.2(6)

This section contains resolved caveats in software Release 3.2(6).

- CSCsg74035

Under certain circumstances, the administrator may not be able to remove the **aaa authentication match** command using the **no aaa authentication match** command to remove it from configuration.

Workaround: Issue “clear configure aaa” to remove all AAA related configuration and re-configure again the required configuration.

- CSCsl76823

FWSMs shipping directly from manufacturing are being shipped with a crashinfo file pre-loaded on the compact flash card. This crashinfo file was not created by the FWSM itself. Instead, it was generated by the FWSM that was used to make the master copy of the compact flash card that is then

used to image all new FWSMs. This issue is completely cosmetic and has no impact to the FWSM itself. How to detect: Examine the output of crash file using the **show crashinfo** command. If all the following conditions are true, then you are affected.

1. The crash occurred in the Thread named “BGP Router.”
For Example: BGP Router (Old pc 0x00112b34 ebp 0x00000000)
2. Following the traceback, the **show version** output (which is contained in the crashinfo file) displays version 3.2(0)0
For example: FWSM Firewall Version 3.2(0)0
3. The same **show version** output indicates the FWSM serial number is SAD0649033Y. This Serial Number is not the actual Serial Number of the FWSM.

Workaround: Enter the **clear crashinfo** command to remove the incorrect crashinfo file from flash.

- 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 13](#) were resolved in software Release 3.2(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 13 Resolved Caveats in Release 3.2(6)

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
CSCsm42519	FWSM crashes in Thread Name: radius_snd
CSCsm50370	ip address command breaks routing with duplicate statics
CSCsm53140	Inconsistency in sysopt tcp window-scale configuration (new CLI)
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

Table 13 *Resolved Caveats in Release 3.2(6) (continued)*

Caveat ID	Description
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
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

Resolved Caveats in Software Release 3.2(5)

This section contains resolved caveats in software Release 3.2(5).

- CSCsj04022

When a user tries to configure class maps containing large access lists and then tries to apply them to policy maps, access list compilation occurs. During compilation, the access list memory space might get exhausted due to FWSM hardware limitations. For example:

```
hostname(config)# class-map test3
hostname(config-cmap)# match access-list 50000
hostname(config-cmap)# policy-map global_policy
hostname(config-pmap)# class test3
hostname(config-pmap-c)# inspect dns
Memory for compiling access rules exhausted, aborting the current compilation and
continuing to use the existing access rules.
```

On the FWSM, compiled access lists are stored in the Network Processor (NP) memory. The error message generated above actually reports about the exhaustion of access list node objects on the NP. The following command shows the nodes in use:

```
hostname(config)# show np 3 acl stats
-----
ACL Tree Statistics
-----
Rule count : 8274
Bit nodes (PSCB's): 14180
Leaf nodes : 14173
Total nodes : 28353 (max 28356) <-- it's close to the limit
Leaf chains : 6394
Total stored rules: 16457
Max rules in leaf : 5
```

Node depth : 23

Access list node memory objects consumed during an unsuccessful access list compilation are expected to be released when the compilation is aborted, but they are not. Thus, the access list node counter is increasing after every unsuccessful compilation attempt. This memory is never released on the NP, preventing the user from configuring and applying new access lists in the system.

Workaround: Do not configure access lists that might reach FWSM limits during compilation. The only way to release leaked access list memory after an aborted compilation is to reload the FWSM.

- CSCsj12745

The **aaa authentication clear-conn** command does not clear inbound ssh/telnet connection after uauth timer is expired. This problem happens when, client from outside first gets authenticated with Virtual telnet/SSH to Virtual telnet/SSH ip address on FWSM and then initiates the successful telnet/ssh session to inside host. The FWSM is configured with the **aaa authentication include telnet/ssh outside** command.

Workaround: User can use the **aaa authentication include tcp/0 outside** command for authentication.

- CSCsj97975

With the maximum number of ACEs configured in a context when a **nameif** command is entered, access list Memory exhaustion messages are seen on the FWSM console.

Workaround: Remove the **nameif** command, then remove some ACEs before re-entering the **nameif** command.

- CSCsk71833

If you remove a **nameif** command, the **match interface** command in an OSPF route map shows as “match interface OSPF Unknown Type” instead of removing the **match interface** statement.

Workaround: Manually remove the **match interface** command.

- CSCsl08131

If you configure the **virtual ssh** command as well as a **static** command for the virtual SSH IP address, then when an SSH login or logout is done to the virtual SSH IP address, it is not reflected in the uauth entry. Further, when uauth entry for the particular user is not present, then during the login authentication the following message is displayed:

```
[root@Linux ~]# ssh -l username virtual_SSH_IP_Addr
LOGIN Authentication                               <<<< LOGIN
username@virtual_SSH_IP_Addr's password:

Logout Successful                                 <<<< LOGOUT
Connection closed by virtual_SSH_IP_Addr
[root@Linux ~]#
```

If the uauth entry for the user is already present, then following message is displayed during the Logout authentication:

```
[root@Linux ~]# ssh -l username virtual_SSH_IP_Addr

LOGOUT Authentication                             <<<< LOGOUT
username@virtual_SSH_IP_Addr's password:

Authentication Successful                         <<<< LOGIN
Connection closed by virtual_SSH_IP_Addr
[root@Linux ~]#
```

Workaround: Use virtual SSH without a **static** NAT statement.

- CSCsI08177

When virtual Telnet and virtual SSH are both configured at the same IP address, virtual Telnet works fine, but virtual SSH stops working.

Workaround: Configure the **virtual ssh** and **virtual telnet** commands at different IP addresses on the FWSM.

The caveats listed in [Table 14](#) were resolved in software Release 3.2(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 14 **Resolved Caveats in Release 3.2(5)**

Caveat ID	Description
CSCsh62757	Crash in thread name: doorbell poll running with router mode
CSCsj81538	FWSM running 3.2(1) has ASR feature broken with transparent mode
CSCsk72522	Unable to add access-list error rc=0xc014
CSCsk76920	FWSM TCP Proxy Fails when TCP Window Scaling is Used
CSCsk95763	fws 3.2.2 - rtsp inspection / malloc failure causes reboot
CSCsl04910	ACL change causes high CPU and possible network outage
CSCsl21097	FWSM re-orders packets with small tcp segment size
CSCsl24414	FWSM:BPDU keep passing through when intf shutdown in transparent context
CSCsl29505	FWSM does not free up RADIUS IDs when there are many rejects
CSCsl29965	FWSM SNMP MIB does not include failover interfaces
CSCsl33529	Stby FWSM passes traffic to other intf during bulk sync cause pkt drops
CSCsl34341	show np 3 flow rate wrong output
CSCsl34625	FWSM crash in assert with c_bridge_group:bridge_group_action
CSCsl48068	system context: login command fails
CSCsl50309	FWSM crashes due to sunrpc inspection
CSCsl52399	FTP inspection inserting incorrect PAT address
CSCsl57262	DHCP discover is dropped by FWSM
CSCsl57838	Config replication under heavy fast-path load causes NP hang
CSCsl65187	FWSM: crash in telnet/ci capture:destroy_capture
CSCsl70414	'write standby' on FWSM reintroduces default policy map on standby
CSCsl80895	Transparent Mode Nat-control by default during 2.3->3.2 upgrade
CSCsl89773	Cos/DSCP of Failover packet is 0, not 5
CSCsl97424	FWSM displays inconsistent value for 'Configuration last modified'
CSCsm01604	Ping command with no destination ip specified causes crash
CSCsm07395	Enabling FTP inspection can introduce out-of-order packets on egress
CSCsm13097	Config replication under heavy fast-path load causes NP hang
CSCsl60126	Converting rpc and rpc_udp fixups to MPF triggers redundant sunrpc
CSCsm38173	Crashing in thread url_filter

Table 14 *Resolved Caveats in Release 3.2(5) (continued)*

Caveat ID	Description
CSCsm27076	SMTP Fixup dropping 64-byte DATA packet that has 4 zeroes of padding
CSCsk00837	Multicontext transparent FW with NAT affects ICMP and UDP traffic.
CSCsk81211	DHCPrelay binding limit of 100 to be configurable for scalability
CSCsm23724	ERROR: vcid 0 belongs to tree 17, yet try to add rules to tree
CSCsm13097	Config replication under heavy fast-path load causes NP hang
CSCsm07395	Enabling FTP inspection can introduce out-of-order packets on egress
CSCsm37177	Implement a mechanism to send queries to websense with context name
CSCsj56795	FWSM slow TCP performance due to packet re-ordering
CSCsl10667	FWSM introduces out of order packets into TCP connections

Resolved Caveats in Software Release 3.2(4)

This section contains resolved caveats in software Release 3.2(4).

- CSCsj01533

With a 32-character password, authentication fails for SSH V1. This is seen with SSH V1 only and not with SSH V2. Authentication fails for a 32-character password only. Authentication works up to 31 characters.

Workaround: Either use SSH V2 or use a password up to 31 character long.

- CSCsj97085

Command authorization using TACACS+ fails for **show running-config nat** and **show running-config static** commands.

Workaround: Use the **show running-config | include nat** and **show running-config | include static** commands, if **show running-config** is permitted.

- CSCsl05935

After configuring the FWSM with a very basic configuration and SNMP-related commands, occasionally the **show perfmon detailed** command shows huge values for Connections in the last 1 minute.

Workaround: None.

The caveats listed in [Table 15](#) were resolved in software Release 3.2(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 15 *Resolved Caveats in Release 3.2(4)*

Caveat ID	Description
CSCsl08519	Application Inspection Vulnerability in Cisco Firewall Services Module
CSCsl30468	FWSM may crash in thread BGP Router
CSCsl41868	FWSM 3.2.3 may reload with traceback and not save a crash file to flash

Table 15 **Resolved Caveats in Release 3.2(4) (continued)**

Caveat ID	Description
CSCsk71799	Standby shows ospf neighbor even after dead time expires
CSCsg33510	SCP communication failed while downloading vlans to FWSM
CSCsk83269	SunRPC fails through FWSM with PAT after upgrade to 3.1
CSCsk73159	FWSM 3.2.2.10: Gatekeeper to Gatekeeper communication is broken
CSCsk80754	FWSM 3.1.7.2: PAT broken for inbound SIP calls
CSCsk95763	fws 3.2.2 - rtsp inspection / malloc failure causes reboot
CSCsk99071	FWSM sends grat. arp on bootup even when interface shutdown

Resolved Caveats in Software Release 3.2(3)

This section contains resolved caveats in software Release 3.2(3).

- CSCsi03932
dACLs downloaded from RADIUS server with uauth sessions are unable to remove from the system with uauth session timeout/deletion and even with the **clear config access-list** command.
Workaround: None.
- CSCsi85092
Sometimes the “Authentication successful” window does not get displayed. The issue is seen only when the credentials are entered after the syslog “%FWSM-5-109012: Authen Session End: user ", sid 24, elapsed 30 seconds” gets displayed. This syslog gets displayed when the pending xlate for the HTTP connection is freed after 30 seconds.
Workaround: None.
- CSCsj87817
After failover, active connections associated with uauth are not cleared when the uauth timer expires.
Workaround: Enter the **clear conn** command to clear the connections.
- CSCsj90829
When trying to authenticate a single user using 4001 dynamic access lists, the active FWSM fails over to the standby unit.
Workaround: Reduce the number of dynamic access lists for the user.
- CSCsj97107
When using command authorization using TACACS+, a user connected to the FWSM can enter into privileged EXEC mode only one time. If the user exits privileged EXEC mode and tries to re-enter privileged EXEC mode (using the **disable** command and then the **enable** command), command authorization fails because the username sent to the TACACS+ server is not the correct username.
Workaround: Close the Telnet session with the FWSM and re-establish a new session.
- CSCsk01392
If you enable URL filtering, HTTP inspection, and DCERPC inspection, and a client uses outlook web access (OWA), the FWSM crashes.
Workaround: Disable URL filtering.

- CSCsk06306

When you configure the **virtual http** command, and a user logs in with a non-existent username and no password, then the FWSM shows a LOGIN successful message, even though the login was not successful.

Workaround: None.

The caveats listed in [Table 16](#) were resolved in software Release 3.2(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 16 *Resolved Caveats in Release 3.2(3)*

Caveat ID	Description
CSCsg48243	Window Scaling dramatically slows HTTP performance
CSCsi63925	Auth proxy generates login form with server IP address instead of name
CSCsj11158	Inconsistency of dACL associated to User in Active&Standby
CSCsj16291	Adding network statement under OSPF doesn't send Withdraw msg for BGP
CSCsj41577	denid traffic with DACL is allowed after fwsm failover
CSCsj45156	BGP doesn't work properly if the link between the BGP peers is broken
CSCsj56579	FWSM shows connection setup rates incorrectly
CSCsj69535	Crash-virtual telnet with radius aaa authentication and dACLs
CSCsj78808	FWSM crash in threadname SSH
CSCsj87299	dACL fails to show in standby unit
CSCsk00270	RTSP inspect only uses first address in PAT pool
CSCsk23005	FWSM - Module does not goes to FAILED state on expiry of hold time
CSCsk25836	MP software does not clear aaa cmds from admin context
CSCsk28118	Assert on standby with dACL / av-pair option
CSCsk28398	TCP Normalizer not aware of tcp window scaling option creating problems
CSCsk29124	FWSM crashed at radius.c after running traffic using dacls
CSCsk34368	Inspect DCERPC failure. Packet too small error
CSCsk35409	Primary assert at radius.c:456
CSCsk35495	TCP state by-pass does not update IDLE timer on established connections
CSCsk45531	crash in bgp_calculate_routerid () at bgp.c
CSCsk46540	Syncing of admin context with BGP resulting in secondary
CSCsk47111	clear uauth removes tcp connection without aaa clear-conn configured
CSCsk47717	Unable to sync config to secondary and results crash
CSCsk54901	NP got stuck after a telnet/http traffic
CSCsk59400	Traceroute through Transparent Context w/xlate-bypass fails
CSCsk59681	On deleting last ACE, access-group is not removed properly
CSCsk59687	ICMP inspection not working with PAT.
CSCsk59831	Connection Not Replicated after write standby in A/S MFM-TFW

Table 16 *Resolved Caveats in Release 3.2(3) (continued)*

Caveat ID	Description
CSCsk59884	Standby Crashed at hash_iter_init
CSCsk61721	With MTU configured, ICMP traffic is not going through
CSCsk61742	TFW: uauth not happening with secure-http-client
CSCsk65721	FWSM reloads while clear config all when management session exists
CSCsk71393	DAACL with deny ACE: Access-1 name is not synced to standby
CSCsk73220	Connections are not cleared after clear uauth
CSCsk79231	NP1/2 Stuck with multicast traffic
CSCsk86440	FWSM traceback on thread fast_fixup

Resolved Caveats in Software Release 3.2(2)

This section contains resolved caveats in software Release 3.2(2).

- CSCsh97363
FWSM will crash while downloading a DAACL with 64 or more aces when debug radius is enabled.
Workaround: Turn off “debug radius”.
- CSCsj17064
Unable to remove resource rule configuration using the **clear config all** command. This condition is seen when trying to remove the **resource rule** command using the **clear config all** command.
Workaround: Use the **clear config resource rule** command or the **no resource rule** command.

The caveats listed in [Table 17](#) were resolved in software Release 3.2(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 17 *Resolved Caveats in Release 3.2(2)*

Caveat ID	Description
CSCsh92146	"Wrong port chosen in xlate creation with STATIC PAT,GW fails to register"
CSCsh97363	FWSM crashed at radius.c
CSCsi77557	Resource rules: Incorrect total max rule count printed
CSCsi77844	http codenomicon crashed fwsm running 3.2(0.75)
CSCsj01513	FWSM: Crash ssh_buffer_append_space found on image 3.2.0.84
CSCsj04140	FWSM fails to download acl with acl length < 3 characters
CSCsj04449	Firewall crash at hash_table_simple.c:267
CSCsj04966	sh uauth shows some junk access-list after failover from active to stand
CSCsj09373	dACL is removed on original active after failover
CSCsj17064	Unable to remove resource rule configuration using clear config all
CSCsj17171	FWSM: Failed adding/deleting Rule to classifier

Table 17 *Resolved Caveats in Release 3.2(2) (continued)*

Caveat ID	Description
CSCsj24249	WAAS traffic stops after add/remove inspect waas in interface policy
CSCsj36646	NP3 assert in ho.lst after failover configured PAT in transparent mode
CSCsj44655	Assert on withPrimary pdp_ptr->magic == GTP_PDP_MAGIC
CSCsj46090	Failover: Primary doesn't get back to Active on rare situation
CSCsj50842	FWSM may traceback in threadname RTSP
CSCsj63745	cannot wr mem when ACL is used in capture command
CSCsj67853	crash after show asp table mac-address-table command
CSCsj69930	FWSM management traffic through vpn allowed even when not configured
CSCsj69977	Ethertype ACL got corrupted after reload
CSCsj82547	repeative telnet to ipv6 address of fws disable telnet access -ddos
CSCsj88848	write standby on active resets the standby module
CSCsj89145	"When Active-Active failover configured, shared vlan devices are not reach"
CSCsj95833	Primary crash in uauth_lookup with uauth traffic
CSCsj35852	Crash in thread name: Doorbell_Poll

Related Documentation

See the following sections for related documentation:

- [Hardware Documents, page 33](#)
- [Software Documents, page 33](#)

Hardware Documents

See the following related hardware documentation:

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

Software Documents

See the following related software documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*

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

Obtaining Documentation, 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

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.

©2009 Cisco Systems, Inc. All rights reserved.