



Release Notes for the Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module, Software Release 2.2(1)

July 29, 2004

These release notes describe the features, modification, and caveats for the Firewall Services Module (FWSM) software release 2.2(1).

Contents

These release notes include the following sections:

- [Important Notes, page 2](#)
- [Chassis System Requirements, page 2](#)
- [Management Support, page 3](#)
- [Limitations and Restrictions, page 8](#)
- [Upgrading the Software, page 8](#)
- [Software License Information, page 8](#)
- [Limitations and Restrictions, page 8](#)
- [Open Caveats in Release 2.2\(1\), page 10](#)
- [Resolved Caveats in Release 2.2\(1\), page 17](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Important Notes

See the following important notes for configuring the FWSM:

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

Chassis System Requirements

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

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

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

Table 1 Support for FWSM 2.2 Features

| | Supervisor Engines ¹ | FWSM Features: | |
|-------------------------|---------------------------------|----------------------------|---|
| | | Multiple SVIs ² | Transparent Firewall with Failover ³ |
| Cisco IOS | | | |
| 12.1(13)E | 2 | No | No |
| 12.1(19)E | 2 | Yes | No |
| 12.1(22)E and higher | 2 | Yes | Yes |
| 12.2(14)SY and higher | 2 | Yes | No |
| 12.2(14)SX | 2, 720 | No | No |
| 12.2(17a)SX3 | 2, 720 | Yes | Yes |
| 12.2(17b)SXA | 2, 720 | Yes | Yes |
| 12.2(17d)SXB and higher | 2, 720 | Yes | Yes |

Table 1 Support for FWSM 2.2 Features

| | Supervisor Engines ¹ | FWSM Features: | |
|--------------------------------|---------------------------------|----------------------------|---|
| | | Multiple SVIs ² | Transparent Firewall with Failover ³ |
| Catalyst OS⁴ | | | |
| 7.5(x) | 2 | No | No |
| 7.6(1) through 7.6(4) | 2 | Yes | No |
| 7.6(5) and higher | 2 | Yes | Yes |
| 8.2(x) | 2, 720 | Yes | Yes |
| 8.3(x) | 2, 720 | Yes | Yes |

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

Management Support

The FWSM supports the following management methods:

- Cisco PDM for FWSM—Release 4.0 supports FWSM Release 2.2 features. PDM is a browser-based configuration tool that resides on the FWSM. The system administrator can configure multiple security contexts. If desired, individual context administrators can configure only their contexts.
- Cisco Firewall MC—Release 1.3.1 supports FWSM Release 2.2 features. For multiple context mode, Release 1.3.1 supports management of each context separately but does not support system-level operations, such as adding or deleting contexts, or the provisioning of failover in multiple mode.
- Command-line interface (CLI)—Access the CLI by sessioning from the switch or by connecting to the FWSM over the network using Telnet or SSH. The FWSM does not have its own external console port.

New Features

Table 2 lists the new features for FWSM release 2.2.

Table 2 New Features

| Feature | Description |
|--|---|
| Transparent firewall or routed firewall mode | <p>The firewall can run in one of the following modes:</p> <ul style="list-style-type: none"> • Routed—The FWSM is considered to be a router hop in the network. It performs NAT¹ between connected networks. In single context mode, you can use OSPF² or passive RIP³. • Transparent—The FWSM acts like a “bump in the wire,” and is not a router hop. The FWSM connects the same network on its inside and outside interfaces, but each interface must be on a different VLAN. No dynamic routing protocols or NAT are required. <p>See the firewall mode command.</p> |
| Multiple security contexts | <p>In multiple context mode, you can create up to 100 separate security contexts (depending on your software license). A security context is a virtual firewall that has its own security policy and interfaces. Multiple contexts are similar to having multiple stand-alone firewalls. Contexts are conveniently contained within a single module.</p> <p>You can run all security contexts in routed mode or in transparent mode; you cannot run some contexts in one mode and others in another.</p> <p>With the default software license, you can run up to two security contexts in addition to a special admin context. For more contexts, you must purchase a license.</p> <p>See the context command.</p> |
| Resource management for security contexts | <p>You can limit resources per context so one context does not use up too many resources. You create classes that define resource limitations as an absolute value or as a percentage, and then assign a context to one of these classes.</p> <p>See the class command.</p> |
| Communication between same security level | <p>You can configure interfaces on the same security level to communicate with each other. This feature is off by default, and you can enable or disable this feature on a per context basis. In earlier releases, no communication between interfaces with the same security level was possible.</p> <p>See the same-security-traffic command.</p> |
| Bidirectional NAT and policy NAT | <p>You can perform NAT on inside and outside addresses. For policy NAT, you can identify addresses to be translated using an extended ACL⁴, which allows you more control in determining which addresses to translate.</p> <p>For outside NAT, see the nat outside command or the static command. For policy NAT, see the nat access-list or static access-list command.</p> |

Table 2 New Features (continued)

| Feature | Description |
|----------------------------|--|
| Several ACL types | <p>The FWSM supports the following ACLs:</p> <ul style="list-style-type: none"> • Extended ACL to control IP traffic on an interface: <ul style="list-style-type: none"> – Inbound – Outbound See the access-list extended command. • For transparent firewall mode, EtherType ACL to control non-IP traffic on an interface: <ul style="list-style-type: none"> – Inbound – Outbound See the access-list ethertype command. • Standard ACL for OSPF route redistribution. <ul style="list-style-type: none"> – Outbound See the access-list standard command. <p>ACL enhancements include:</p> <ul style="list-style-type: none"> • Comments in ACLs. <ul style="list-style-type: none"> – See the access-list remark command. • System messages when traffic matches an ACE⁵. <ul style="list-style-type: none"> – See the log keyword for the access-list command. |
| DHCP server and DHCP relay | <p>The FWSM acts as a DHCP⁶ server. The FWSM also supports DHCP relay to forward DHCP requests to an upstream router. The DHCP server supports options in DHCP requests, including option 150 and option 66 for VoIP⁷ applications.</p> <p>See the dhcpd and dhcprelay commands.</p> |
| Login banners | <p>You can define a text message to display when users log into the FWSM.</p> <p>See the banner command.</p> |
| Failover enhancements | <p>The FWSM supports the following failover enhancements:</p> <ul style="list-style-type: none"> • Per-interface monitoring (up to 250 interfaces) and configurable failure threshold. <ul style="list-style-type: none"> – See the monitor-interface command and the failover interface-policy command. • Shorter configurable poll interval. <ul style="list-style-type: none"> – See the failover polltime command. • Configurable holdtime, which sets the time threshold for the standby unit to become active when a unit failure is detected. <ul style="list-style-type: none"> – See the failover polltime holdtime command. • Zero downtime when upgrading to a maintenance release. For example, you can upgrade from 2.2(1) to 2.2(2) without disabling failover even though the software release number does not match exactly on both units. |

Table 2 *New Features (continued)*

| Feature | Description |
|--------------------------------|--|
| System message enhancements | <p>The FWSM supports the following system message enhancements:</p> <ul style="list-style-type: none"> • ACLs can generate system messages when they match traffic. See the log keyword for the access-list command. • You can set the level for a system message. See the logging message level command. • System messages are now compatible with CiscoWorks RME⁸ (emblem format). See the logging host format emblem command. • You can include the hostname in the system message. See the logging device-id command. |
| Inspection engine enhancements | <p>The FWSM supports the following inspection engine enhancements:</p> <ul style="list-style-type: none"> • MGCP⁹ inspection engine support. See the fixup protocol mgcp command. • H.323 inspection engine support for Versions 3 and 4. See the fixup protocol h323 command. • ICMP¹⁰ inspection engine support. See the fixup protocol icmp command. • ICMP error inspection engine support. See the fixup protocol icmp error command. • Sun RPC¹¹ over TCP inspection engine support. This inspection engine supports services such as NFS¹² or NIS+¹³. See the fixup protocol rpc command and the rpc-server command. • DNS¹⁴ inspection engine support. See the fixup protocol dns command. • PAT¹⁵ support for the H.323, Skinny, and SIP inspection engines. |
| Filtering enhancements | <p>The FWSM supports the following filtering enhancements:</p> <ul style="list-style-type: none"> • HTTPS¹⁶ filtering (Websense only). See the filter https command. • FTP¹⁷ filtering (Websense only). See the filter ftp command. • N2H2 support for HTTP¹⁸ filtering. |

Table 2 *New Features (continued)*

| Feature | Description |
|---------------------------------|--|
| AAA ¹⁹ enhancements | <p>The FWSM supports the following AAA enhancements:</p> <ul style="list-style-type: none"> • Fallback to the local database when the server is unreachable for CLI authentication, enable authentication, command authorization, or VPN²⁰ authentication. • Downloadable ACLs per user from a RADIUS²¹ server. |
| SNMP ²² enhancements | <p>The FWSM supports the following SNMP enhancements:</p> <ul style="list-style-type: none"> • You can change the UDP²³ port on which traps are sent to the server. See the udp-port keyword in the snmp-server command. • You can specify traps to be sent by feature and name. See the snmp-server enable traps command. • Cisco Firewall MIB²⁴ support <ul style="list-style-type: none"> – cfwEvents – cfwSecurityNotification trap • Cisco Process MIB support—cpmCPUTotalTable. The CPU usage described in this table applies only to the FWSM general-purpose processor, and not to the network processors. |

1. Network Address Translation
2. Open Shortest Path First
3. Routing Information Protocol
4. access control lists
5. Access Control Entry
6. Dynamic Host Configuration Protocol
7. Voice over IP
8. Resource Management Essentials
9. Media Gateway Control Protocol
10. Internet Control Message Protocol
11. Remote Procedure Call
12. Network File System
13. Network Information Service+
14. Domain Name Service
15. port address translation
16. HyperText Transfer Protocol over SSL
17. File Transfer Protocol
18. HyperText Transfer Protocol
19. authentication, authorization, and accounting
20. Virtual Private Network
21. Remote Authentication Dial-In User Service
22. Simple Network Management Protocol
23. User Datagram Protocol
24. Management Information Base

Upgrading the Software

The following command allows you to upgrade from Release 1.1 (or pre-release versions of 2.x) to Release 2.2. For other upgrade options for upgrading from Release 2.x, such as upgrading to a different application partition or from a different type of server, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

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

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

For example, enter the following command:

```
FWSM# copy tftp://209.165.200.226/cisco/c6svc-fwm-k9.2-1-1.bin flash:
```

Software License Information

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

Limitations and Restrictions

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

- [Limitations and Restrictions on the FWSM, page 9](#)
- [Limitations and Restrictions in Cisco IOS Software, page 9](#)
- [Limitations and Restrictions in Catalyst OS, page 10](#)

Limitations and Restrictions on the FWSM

See the following limitations and restrictions on the FWSM:

- Multiple context mode does not support dynamic routing protocols such as RIP and OSPF. Use static routing instead.
- Transparent firewall mode supports a maximum of two interfaces per context.
- For transparent firewall mode, you must configure a management IP address.
- Outbound connections (from a higher security interface to a lower security interface) from an interface that is shared between 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 generally unsupported, because configuring static translations for all outside hosts is typically not feasible.
- There might be commands that are CPU intensive and could affect the system performance. Therefore, we suggest that you perform actions such as loading a large configuration or compiling a large ACL with caution.

Limitations and Restrictions in Cisco IOS Software

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

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

Limitations and Restrictions in Catalyst OS

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

- Although the FWSM can handle jumbo Ethernet frames, the switch does not handle jumbo frames through the FWSM. See caveat CSCee03625 for more information.
- If you reload the switch or the FWSM, the switch might lose the configuration that assigns VLANs to the FWSM. You need to re-enter the **set vlan firewall-vlan** command after the reload. See caveat CSCed69941 for more information. This problem is resolved in Release 8.3(1), and might be resolved in earlier versions.
- If you reload the switch, the switch might lose the configuration for SVIs on the MSFC. You need to re-enter the **interface vlan** command on the MSFC after the reload. See caveat CSCed69931 for more information. This problem was found in Release 7.6(5) and might exist in later releases as well.

Open Caveats in Release 2.2(1)

See the following sections for open caveats in Release 2.2(1):

- [AAA Caveats, page 10](#)
- [Connection Caveats, page 11](#)
- [Display Caveats, page 12](#)
- [Failover Caveats, page 13](#)
- [NAT Caveats, page 14](#)
- [System Message and SNMP Caveats, page 14](#)
- [Voice Over IP Caveats, page 15](#)
- [Miscellaneous Caveats, page 16](#)

AAA Caveats

- CSCed30210, CSCed31179

If you configure authentication for traffic through the FWSM, and a user triggers authentication using HTTP, then the HTTP GET request fails if it is segmented into more than one packet and the browser receives an HTTP 404-Not Found message. Similarly, if you are filtering HTTP requests using a Websense server, the lookup request to the Websense server fails and you see the following error message: websense encryption is not supported. This problem only occurs when the HTTP request initially triggers authentication.

Workaround: Refresh the browser.

- CSCed83182

If a user authenticates with RADIUS for a management connection to the FWSM, and you configure a downloadable ACL on the RADIUS server for the user, then the FWSM downloads the ACL but fails to bind it to the user authentication session. If the user sends traffic through the FWSM while this authentication session is active, the ACL will not be in effect, and the user will have unrestricted

access (according to the ACL associated with the interface). Also, because the ACL is not bound to the session, when the session times out, the ACL is not removed from the running configuration. This ACL uses up memory on the FWSM.

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

- CSCed83385

In routed mode, you must add **static** statements for the **virtual telnet** and **virtual http** IP addresses when they are on any interface, and not just when they are on an outside interface. Otherwise, the FWSM fails to respond to ARP requests for these addresses and also fails to create translation sessions.

Workaround: Add a **static** statement specifying the interface connected to the virtual IP address network as the global interface. Any other interface can be used for the local interface. Specify the virtual address as the global address, and any IP address not in use for the local address. For example, if you configure **virtual telnet 10.5.5.5**, and this address is connected to the inside interface network, then create the following **static** statement:

```
static (outside,inside) 10.5.5.5 10.6.6.6 netmask 255.255.255.255
```

- CSCee37328

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

Workaround: The connection eventually goes through.

- CSCee46135

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

Workaround: Configure ACLs on the FWSM and then download the ACL name from the RADIUS server.

Connection Caveats

- CSCec02764

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

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

- CSCec44081

The ILS inspection engine supports only one ILS message per TCP segment. If the ILS server encapsulates multiple ILS messages within one TCP segment, the FWSM interprets them as a single message, causing a parsing error. Also, the FWSM does not perform NAT on this type of packet.

Workaround: None.

- CSCed43330

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

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

- CSCed88264

When you enable same security level communication and set connection limits for an interface in an identity NAT or NAT exemption statement, then the FWSM counts connections toward the maximum connection limit only for traffic inbound to the interface, and not for traffic in both directions.



Note NAT exemption is not currently working according to CSCee32145.

Workaround: None.

- CSCed90656

If you configure a static PAT statement to change UDP DNS port 53 to another port, and you enabled the DNS inspection engine (on by default), then the connection is not allowed because the FWSM applies the DNS Guard protection feature to the connection.

Workaround: None.

- CSCee20506

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

Workaround: None.

- CSCee47998

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

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

Display Caveats

- CSCeb00636

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

Workaround: None.

- CSCee25850

In manual commit mode for ACLs, the **show access-list** command shows standard (OSPF) ACLs as not being committed. The display is incorrect, and the standard ACLs behave as expected.

Workaround: None.

Failover Caveats

- CSCec68302

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

Workaround: None.
- CSCed51205

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

Workaround: Do not use manual commitment (set the **access-list mode auto-commit** command) on the active unit, at least while the standby unit is synchronizing the configuration. Or, after the standby unit syncs, enter the **access-list commit** command on the standby unit to commit all ACLs.
- CSCee10485

When there is a high rate of RTSP traffic, and the RTSP inspection engine is enabled, the FWSM fails to replicate the configuration to the standby unit.

Workaround: Disable the RTSP inspection engine using the **no fixup protocol rtsp** command.
- CSCee24631

In single context mode, when you replicate the configuration to the standby unit, the standby unit RSA key becomes invalid.

Workaround: After synchronization, regenerate the RSA key on the standby unit.
- CSCee31514

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

Workaround: Do not configure the standby unit while you are configuring the active unit; the standby unit should get all its configuration through the replication process. Configuring the standby unit causes the units to get out of sync.
- CSCee47137

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

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

NAT Caveats

- CSCea75037
If you configure a **static** command using the **interface** keyword to specify the interface address, if you change the interface IP address, the change is not reflected in the static translation.
Workaround: None.
- CSCed78642
If you configure the **dns** option in a **static** statement, and the **static** statement specifies a network instead of a single host, then in some cases, the DNS reply is translated to the network address instead of the corresponding host address.
Workaround: None.
- CSCee28447
If you erroneously configure **static** statements in two contexts that identify the same global address on a shared interface (such as the outside interface), neither static statements work. If you delete one statement, the remaining statement still does not work.
Workaround: Remove both static statements, and reconfigure them correctly.
- CSCee32145
When you configure same security interfaces, NAT exemption statements (**nat 0 access-list**) are ignored. You might use NAT exemption statements to set connection limits when you do not want to perform address translation.
Workaround: Use identity NAT (**nat 0**) or static identity NAT.
- CSCee48769
When you configure the embryonic limit for an inside **static** statement, and you also configure dynamic PAT for an outside interface, then a SYN attack from the outside to the inside static address causes a large number of PAT translations with associated connections, even though the connections are not established. These PAT translations do not time out within the default 30 second interval for translations without associated connections because the FWSM thinks there are valid connections associated. The pool of addresses and ports for the outside addresses gets used up, and no additional clients can connect.
Workaround: Do not configure outside PAT if you want to protect the inside address from a SYN attack using an embryonic limit.

System Message and SNMP Caveats

- CSCed92496
When a smurf attack occurs against the FWSM, the FWSM correctly drops the traffic, but does not generate a system message or SNMP trap about the smurf attack.
Workaround: None.
- CSCee22063
When a Land Attack is issued against the FWSM, a system message displays (106017), but no SNMP trap is sent.
Workaround: None.

- CSCee27445
When you configure ACL logging, and you reach the maximum number of deny flows several times, the maximum deny flow system message (106101) continues to be generated even when the maximum is not reached.
Workaround: None.
- CSCee29967
In multiple context mode, the system execution space cannot send system messages to an external syslog server through the admin context; you can only view these system messages from the buffer or on your session monitor.
Workaround: None.
- CSCee50131
All ACLs have an implicit deny at the end consisting of **deny ip any any**. When a packet is dropped because of the implicit deny, the FWSM does not generate the system message 106023 that indicates when a packet is dropped by an ACL.
Workaround: Add an ACE consisting of **deny ip any any** at the end of the ACL. When you have an explicit ACE, you can set additional logging options as well.
- CSCin72275
When the maximum number of deny flows is reached for ACE logging, the FWSM generates system message 10601. However, if you set the alert interval for this message to be greater than the default 300 seconds, then the FWSM does not generate the message.
Workaround: Set the **access-list alert-interval** command to be 300 seconds or less.

Voice Over IP Caveats

- CSCdw13911
The FWSM drops segmented H.323, SIP, and Skinny messages.
Workaround: If both signaling devices are Cisco routers, then you can enter the following command on each router: **ip tcp path-mtu-discovery**. This command might resolve the segmentation if it is caused by the use of TCP MSS=536 by the router. Check the value of the TCP MSS by looking at the first two packets of the connection in a sniffer program.
- CSCec11628
Inter-cluster Cisco CallManager (3.3) trunks, connected without the use of Gatekeepers (one Cisco CallManager connected directly to another Cisco CallManager), often experience delayed or disrupted call setup and voice path connections. The majority of calls are successful.
Workaround: Use either Gatekeeper-controlled inter-cluster trunks, or use Cisco CallManagers on two FWSM interfaces of the same security level.
- CSCed02843
If you configure PAT, the FWSM might not translate the IP address in the “o” (owner) header of the SDP packet to the PAT address. This problem occurs when the Cisco IOS gateway is on the inside interface and the proxy server and phones are on the outside. This symptom does not occur if the phone is a 79xx SIP phone.
Workaround: None.

- CSCed83014
When the FWSM is between a Cisco CallManager (with SCCP phones registered) and an H.323 gateway (with plain old telephone service (POTS) phones attached), VoIP calls between a SCCP phone and a POTS phone sometimes fails.
Workaround: None.
- CSCee14284
If you configure two interfaces on the same security level and you configure PAT for both inside interfaces when they access the outside, then if both interfaces have a SIP phone with the proxy on the outside, a SIP call between the two same security interfaces fails. The ACK is dropped by the FWSM.
Workaround: Do not use PAT in this situation; use NAT instead.
- CSCee14294
If two contexts share an outside interface, and SIP phones on each context call each other, the INVITE, 100, 180 and 200 messages are handled properly; however, the ACK message does not have all address fields modified in the SIP payload, and the call fails.
Workaround: Do not share the outside interface between contexts with SIP phones.

Miscellaneous Caveats

- CSCdz11283
Because the FWSM does not allow Telnet to the lowest security interface, if you configure a context with only one interface, you cannot Telnet to it because it is inherently the lowest security interface.
Workaround: Configure a second interface at a lower security level, and then delete the interface; the FWSM now allows Telnet to the one remaining interface.
- CSCea93521
If you change any **crypto map** commands, the changes are made in the configuration, but the FWSM still uses the old settings.
Workaround: Reapply the crypto map to the interface by entering the **no crypto map interface** command to remove it, and then re-add it.
- CSCee25902
After you reboot the FWSM, the FWSM might not be able to load all the ACLs in a given context, and you see the following error:

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


This memory problem occurs because contexts are assigned to one of 12 memory pools at startup or when the context is first added. The amount of memory a context can use for ACLs depends on how many contexts share the pool and how many ACLs each context uses. Each time you restart the FWSM, the contexts are distributed evenly across all pools; however, the distribution across pools might differ from the original distribution when you first added a context, resulting in (more or) less memory being available.
Workaround: Because the pool allocation is based on an internal context ID, you might try deleting and re-adding the context in the hopes that its new ID will cause the FWSM to assign it to a less populated pool.

- CSCee30691

In transparent firewall mode, if you enter the **no nameif** command for one of the interfaces while the other interface is shut down, then the FWSM cannot perform the **no nameif** action and shows the following message:

```
Could not add PC mac entry for vPifNum: 4
```

Workaround: Make sure both interfaces are active before you enter the **no nameif** command.

- CSCee41620

When you use Cisco VPN client Release 3.6.3 for management access in routed firewall mode, you cannot use the local database for user authentication.

Workaround: Use RADIUS or TACACS+ for authentication.

- CSCee52559

If you upgrade from Release 1.1 to Release 2.2(1), and you configured an OSPF cost for the failover interface, then the FWSM crashes.

Workaround: Before you upgrade, remove the OSPF cost configuration from the failover interface.

Resolved Caveats in Release 2.2(1)

The following caveats are resolved in Release 2.21:

- CSCec03643

Resolved

When making calls using gateways to the SIP (SMDS Interface Protocol) proxy, UDP and TCP proxy calls fail to set up, or there is no voice path.

Workaround: Do not use gateways with the SIP proxy. SIP Proxy Gateway calls for both UDP & TCP fail to setup or no voice path.

- CSCec07318

Resolved

The NFS mount takes a long time to succeed or fails because the NFS client is on a lower security interface relative to the NFS server.

Workaround: Configure the NFS client on a higher security interface relative to the NFS server.

- CSCec19761

Resolved

Outbound TFTP requests fail if PAT is using an interface IP address that is configured on the FWSM. The TFTP file download works correctly with other PAT IP addresses.

Workaround: None.

- CSCec24882

Resolved

During failover interface testing when the shutdown command is sent manually, testing continues, and the interface state is reported as “unknown.” The interface status should be reported as “Link Down,” and the test should not be performed on the interfaces.

Workaround: None.

Related Documentation

See the following sections for related documentation:

- [Hardware Documents, page 18](#)
- [Software Documents, page 18](#)

Hardware Documents

See the following related hardware documentation:

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

Software Documents

See the following related software documentation:

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

Obtaining Documentation and Submitting a Service Request

For information about 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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)