Monitoring and Troubleshooting the Firewall Services Module

This chapter describes how to monitor and troubleshoot the Firewall Services Module (FWSM), and contains the following sections:

Monitoring the Firewall Services Module

You can monitor the FWSM using system messages or using Simple Network Management Protocol (SNMP). This section describes:

Using System Messages

The FWSM provides extensive system messages. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Messages Guide* to configure logging and to view system message descriptions.

Using SNMP

This section describes how to use SNMP and includes the following topics:

SNMP Overview

The FWSM provides support for network monitoring using SNMP V1. The FWSM supports traps and SNMP get requests, but does not support SNMP set requests.

You can configure the FWSM to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the Management Information Bases (MIBs) on the FWSM. MIBs are a collection of definitions, and the FWSM maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1, MIB-II compliant browser to receive SNMP traps and browse a MIB.

Table 17-1 lists supported MIBs and traps for the FWSM and, in multiple mode, for each context. You can download Cisco MIBs from the following website:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

After you download the MIBs, compile them for your NMS.

Table 17-1 SNMP MIB and Trap Support

MIB or Trap Support	Description
SNMP core traps	The FWSM sends the following core SNMP traps: • authentication—An SNMP request fails because the NMS did not authenticate with the correct community string. • linkup—A VLAN interface is up. • linkdown—A VLAN interface is down, for example, if you removed the **nameif** command, or the VLAN was removed from the switch configuration. • coldstart—The FWSM is running after a reload.
MIB-II	The FWSM supports browsing of the following groups and tables: • system • interfaces • ip.ipAddrTable
Cisco Firewall MIB	The FWSM supports browsing of the following groups: • cfwEvents • cfwSystem The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context. The FWSM supports the following trap: • cfwSecurityNotification
Cisco Memory Pool MIB	The FWSM supports browsing of the following table: • ciscoMemoryPoolTable—The memory usage described in this table applies only to the FWSM general-purpose processor, and not to the network processors.
Cisco Process MIB	The FWSM supports browsing of the following table: • cpmCPUTotalTable—The CPU usage described in this table applies only to the FWSM general-purpose processor, and not to the network processors.
Cisco Syslog MIB	The FWSM supports the following trap: • clogMessageGenerated You cannot browse this MIB.

Enabling SNMP

The SNMP agent that runs on the FWSM performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the FWSM, follow these steps:

Step 1 To identify the IP address of the NMS that can connect to the FWSM, enter the following command:

```
FWSM/contexta(config)# snmp-server host interface_name ip_address [trap | poll]
[udp-port port]
```

Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.

SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port** keyword.

Step 2 To specify the community string, enter the following command:

```
FWSM/contexta(config)# snmp-server community key
```

The SNMP community string is a shared secret between the FWSM and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default is **public**.

Step 3 (Optional) To set the SNMP server location or contact information, enter the following command:

```
FWSM/contexta(config)# snmp-server {contact | location} text
```

Step 4 To enable the FWSM to send traps to the NMS, enter the following command:

```
FWSM/contexta(config)# snmp-server enable traps [all | syslog | firewall | snmp [trap1]
[trap2] [...]]
```

By default, SNMP core traps are enabled (**snmp**). If you do not enter a trap type in the command, **syslog** is the default. To enable or disable all traps, enter the **all** option. For **snmp**, you can identify each trap type separately. See Table 17-1 on page 17-2 for a list of traps.

Step 5 To enable system messages to be sent as traps to the NMS, enter the following command:

```
FWSM/contexta(config)# logging history level
```

You must also enable **syslog** traps using the **snmp-server enable traps** command above.

Step 6 To enable logging, so system messages are generated and can then be sent to an NMS, enter the following command:

```
FWSM/contexta(config)# logging on
```

The following example sets the FWSM to receive requests from host 192.168.3.2 on the inside interface, but the FWSM does not send SNMP traps.

```
FWSM/contexta(config)# snmp-server host 192.168.3.2
FWSM/contexta(config)# snmp-server location building 42
FWSM/contexta(config)# snmp-server contact kim lee
FWSM/contexta(config)# snmp-server community ohwhatakeyisthee
```

Troubleshooting the Firewall Services Module

This section describes how troubleshoot the FWSM, and includes the following topics:

Testing Your Configuration

This section describes how to test connectivity for the single mode FWSM or for each security context. The following steps describe how to ping the FWSM interfaces, and how to allow hosts on one interface to ping through to hosts on another interface.

We recommend that you only enable pinging and debug messages during troubleshooting. When you are done testing the FWSM, follow the steps in the "Disabling the Test Configuration" section on page 17-8.

This section includes:

Enabling ICMP Debug Messages and System Messages

Debug messages and system messages can help you troubleshoot why your pings are not successful. The FWSM only shows ICMP debug messages for pings to the FWSM interfaces, and not for pings through the FWSM to other hosts. To enable debugging and system messages, follow these steps:

Step 1 To show ICMP packet information for pings to the FWSM interfaces, enter the following command:

```
FWSM/contexta(config)# debug icmp trace
```

Step 2 To set system messages to be sent to Telnet or SSH sessions, enter the following command:

```
FWSM/contexta(config)# logging monitor debug
```

You can alternately use **logging buffer debug** to send messages to a buffer, and then view them later using the **show logging** command.

Step 3 To send the system messages to your Telnet or SSH session, enter the following command:

```
FWSM/contexta(config)# terminal monitor
```

Step 4 To enable system messages, enter the following command:

```
FWSM/contexta(config)# logging on
```

The following example shows a successful ping from an external host (209.165.201.2) to the FWSM outside interface (209.165.201.1):

```
FWSM/contexta(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

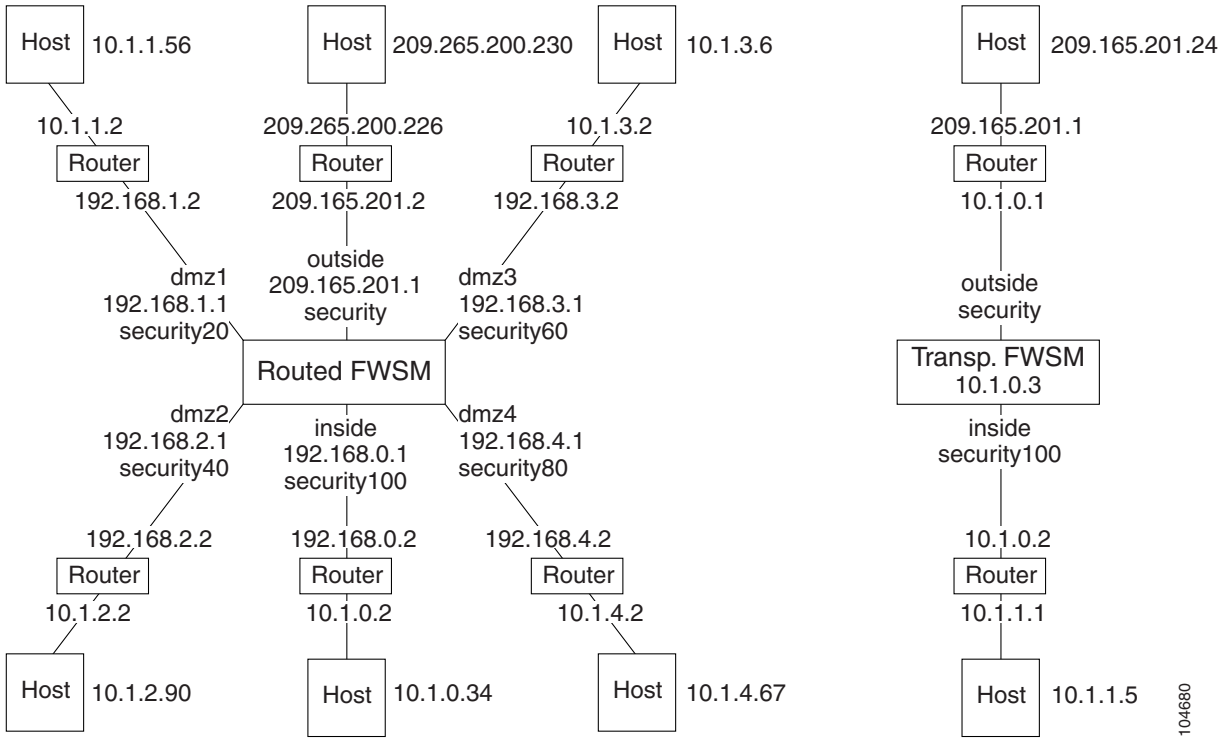
The above example shows the ICMP packet length (32 bytes), the ICMP packet identifier (1), and the ICMP sequence number (the ICMP sequence number starts at 0 and is incremented each time a request is sent).

Pinging FWSM Interfaces

To test that the FWSM interfaces are up and running and that the FWSM and connected routers are routing correctly, you can ping the FWSM interfaces. To ping the FWSM interfaces, follow these steps:

Step 1 Create a sketch of your single mode FWSM or security context showing the interface names, security levels, and IP addresses. The sketch should also include any directly connected routers, and a host on the other side of the router from which you will ping the FWSM. You will use this information for this procedure as well as the procedure in the "Pinging Through the FWSM" section on page 17-7. For example:

Figure 17-1 Network Sketch with Interfaces, Routers, and Hosts



Step 2 To enable ICMP to the FWSM, enter the following command:

```
FWSM/contexta(config)# icmp permit any interface_name
```

Enter this command for each interface you want to test.

Step 3 Ping each FWSM interface from the *directly connected* routers. For transparent mode, ping the management IP address.

This test ensures that the FWSM interfaces are active and that the VLAN configuration is correct.

A ping might fail if the FWSM interface is not active, the VLAN configuration is incorrect, or if a switch between the FWSM and router is down (see Figure 17-2). In this case, no debug messages or system messages appear on the FWSM, because the packet never reaches it.

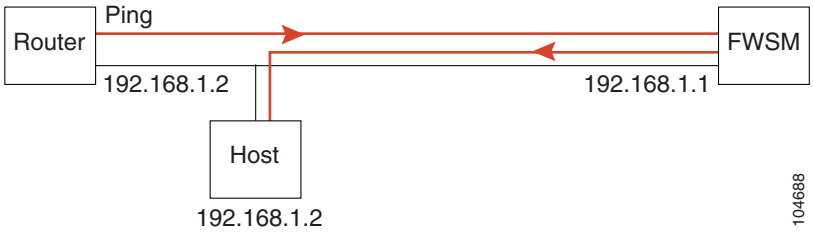
Figure 17-2 Ping Failure at FWSM Interface

If the ping reaches the FWSM, and the FWSM responds, you see debug messages like the following:

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

If the ping reply does not return to the router, then you might have a switch loop or redundant IP addresses (see Figure 17-3).

Figure 17-3 Ping Failure Because of IP Addressing Problems

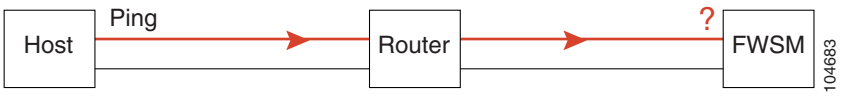


Step 4 Ping each FWSM interface from a remote host. For transparent mode, ping the management IP address.

This test checks that the directly connected router can route the packet between the host and the FWSM, and that the FWSM can correctly route the packet back to the host.

A ping might fail if the FWSM does not have a route back to the host through the intermediate router (see Figure 17-4). In this case, the debug messages show that the ping was successful, but you see system message 110001 indicating a routing failure.

Figure 17-4 Ping Failure Because the FWSM has no Route



Pinging Through the FWSM

After you successfully ping the FWSM interfaces, you should make sure traffic can pass successfully through the FWSM. For routed mode, this test shows that NAT is working correctly. For transparent mode, which does not use NAT, this test confirms that the FWSM is operating correctly; if the ping fails in transparent mode, contact technical support.

You should originate pings from hosts that are normally allowed to access remote networks; you do not need to ping from outside to inside, for example, if you do not allow any outside hosts to access the inside.

To ping between hosts on different interfaces, follow these steps:

Step 1 To add an ACL allowing ICMP from any source host, enter the following command:

```
FWSM/contexta(config)# access-list ICMPTEST extended permit icmp any any
```

Step 2 To assign the ACL to each source interface, enter the following command:

```
FWSM/contexta(config)# access-group ICMPTEST in interface interface_name
```

Repeat this command for each source interface.

Step 3 To enable the ICMP inspection engine, so ICMP responses are allowed back to the source host, enter the following command:

```
FWSM/contexta(config)# fixup protocol icmp
```

Alternatively, you can also apply the ICMPTEST ACL to the destination interface to allow ICMP traffic back through the FWSM.

Step 4 Ping from the host or router through the source interface to another host or router on another interface.

Repeat this step for as many interface pairs as you want to check.

If the ping succeeds, you see a system message confirming the address translation for routed mode (305009 or 305011) and that an ICMP connection was established (302020). You can also enter the **show xlate** and **show conns** commands to view this information.

If the ping fails for transparent mode, contact technical support.

For routed mode, the ping might fail because NAT is not configured correctly (see Figure 17-5). In this case, you see a system message showing that the NAT translation failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation, you see message 106010: deny inbound icmp.

Note The FWSM only shows ICMP debug messages for pings to the FWSM interfaces, and not for pings through the FWSM to other hosts.

Figure 17-5 Ping Failure Because the FWSM is not Translating Addresses

Disabling the Test Configuration

After you complete your testing, disable the test configuration that allows ICMP to and through the FWSM and that prints debug messages. If you leave this configuration in place, it can pose a serious security risk. Debug messages also slow the FWSM performance.

To disable the test configuration, follow these steps:

Step 1 To disable ICMP debug messages, enter the following command:

```
FWSM/contexta(config)# no debug icmp trace
```

Step 2 To disable logging, if desired, enter the following command:

```
FWSM/contexta(config)# no logging on
```

Step 3 To disable ICMP to the FWSM for all interfaces, enter the following command:

```
FWSM/contexta(config)# clear icmp
```

If you want to disable ICMP for a certain interface, use the **no icmp permit** *interface_name* command.

Step 4 To remove the ICMPTEST ACL, and also delete the related **access-group** commands, enter the following command:

```
FWSM/contexta(config)# no access-list ICMPTEST
```

Step 5 (Optional) To disable the ICMP inspection engine, enter the following command:

```
FWSM/contexta(config)# no fixup protocol icmp
```

Reloading the Firewall Services Module

If you need to reload the FWSM, see the following sections:

- Reloading the FWSM from the FWSM CLI, page 17-8
- Reloading the FWSM from the Switch, page 17-9

Reloading the FWSM from the FWSM CLI

In multiple mode, you can only reload from the system execution space. To reload the FWSM from the FWSM CLI, enter the following command:

```
FWSM# reload
```

Reloading the FWSM from the Switch

If you need to reload the FWSM from the switch into the current partition, enter the command for your operating system. See the "Resetting the FWSM or Booting from a Specific Partition" section on page 2-13 for other options.

- For Cisco IOS software, enter the following command:

```
Router# hw-module module mod_num reset
```

- For Catalyst OS, enter the following command:

```
Console> (enable) reset mod_num
```

Troubleshooting Passwords and AAA

If you forget passwords, or you create a lockout situation because of AAA settings, the following sections describe how to recover:

Clearing the Application Partition Passwords and AAA Settings

If you forget the login and enable passwords, or you create a lockout situation because of AAA settings, you can reset the passwords and portions of AAA configuration to the default values. You must log into the maintenance partition to perform this procedure:

Step 1 To boot the FWSM into the maintenance partition, enter the command for your operating system:

- For Cisco IOS software, enter the following command:

```
Router# hw-module module mod_num reset cf:1
```

- For Catalyst OS, enter the following command:

```
Console> (enable) reset mod_num cf:1
```

Step 2 To session into the FWSM, enter the command for your operating system:

- For Cisco IOS software, enter the following command:

```
Router# session slot mod_num processor 1
```

- For Catalyst OS, enter the following command:

```
Console> (enable) session mod_num
```

Step 3 To log into the maintenance partition as root, enter the following command:

```
Login: root
```

Step 4 Enter the password at the prompt:

```
Password: password
```

By default, the password is "cisco."

Step 5 To clear the login and enable passwords, as well as the **aaa authentication console** and **aaa authorization command** commands, enter the following command:

```
root@localhost# clear passwd cf:{4 | 5}
```

Step 6 Follow the screen prompts, as follows:

```
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
        enable password 8Ry2YjIyt7RRXU24 encrypted
        passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration?
[yn] y
Passwords and aaa commands have been erased.
```

Recovering the Maintenance Partition Passwords

If you forget the passwords for the maintenance partition, you can reset them to the default values. You must be logged into the application partition. In multiple mode, you can only reset the passwords from the system execution space.

To reset the maintenance passwords, enter the following command:

```
FWSM# clear mp-passwd
```

Other Troubleshooting Tools

The FWSM provides other troubleshooting tools to be used in conjunction with technical support:

- Viewing Debug Messages, page 17-10
- Capturing Packets, page 17-10
- Viewing the Crash Dump, page 17-11

Viewing Debug Messages

Debug messages can slow the FWSM performance considerably. However, if you are troubleshooting the FWSM, debug messages can be useful. We recommend contacting technical support to help you debug your FWSM. To enable debug messages, see the **debug** commands in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

Capturing Packets

Capturing packets is sometimes useful when troubleshooting connectivity problems or monitoring suspicious activity. The FWSM can track packet information for traffic that passes through the general-purpose processor, including management traffic and inspection engines. The FWSM cannot capture traffic that goes through the network processors (such as most through traffic). We recommend contacting technical support if you want to use the packet capture feature. See the **capture** command in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

Viewing the Crash Dump

If the FWSM crashes, you can view the crash dump information. We recommend contacting technical support if you want to interpret the crash dump. See the **show crashdump** command in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

Common Problems

This section describes common problems with the FWSM, and how you might resolve them.

Symptom When you reset the FWSM from the switch CLI, the system always boots into the maintenance partition.

Possible Cause The default boot partition is set to cf:1.

Recommended Action Change the default boot partition according to the "Setting the Default Boot Partition" section on page 2-13.

Symptom You are unable to log into the maintenance partition with the same password as the application partition.

Possible Cause The application partition and the maintenance partition have different password databases.

Recommended Action Use the password appropriate for your partition. See the "Changing the Passwords" section on page 6-1 for more information.

Symptom Traffic does not pass through the FWSM.

Possible Cause The VLANs are not configured on the switch or are not assigned to the FWSM.

Recommended Action Configure the VLANs and assign them to the FWSM according to the "Assigning VLANs to the Firewall Services Module" section on page 2-2.

Symptom You cannot configure a VLAN interface within a context.

Possible Cause You did not assign that VLAN to the context.

Recommended Action Assign VLANs to contexts according to the "Configuring a Security Context" section on page 5-17.

Symptom You cannot add more than one switched virtual interface (SVI) to the MSFC.

Possible Cause You did not enable multiple SVIs.

Recommended Action Enable multiple SVIs according to the "Adding Switched Virtual Interfaces to the MSFC" section on page 2-5.

Symptom The context configuration was not saved, and was lost when you reloaded.

Possible Cause You did not save each context within the context execution space. If you are configuring contexts at the command line, you did not save the context before you changed to the next context.

Recommended Action Save each context within the context execution space using the **copy run start** command. You cannot save contexts from the system execution space.

Symptom You cannot make a Telnet connection or SSH to the FWSM interface.

Possible Cause You did not enable Telnet or SSH to the FWSM.

Recommended Action Enable Telnet or SSH to the FWSM according to the "Allowing Telnet" section on page 11-1 or the "Allowing SSH" section on page 11-2.

Symptom You cannot ping the FWSM interface.

Possible Cause You did not enable ICMP to the FWSM.

Recommended Action Enable ICMP to the FWSM according to the "Allowing ICMP to and from the FWSM" section on page 11-10.

Symptom You cannot ping through the FWSM, even though the ACL allows it.

Possible Cause You did not enable the ICMP inspection engine or apply ACLs on both the source and destination interfaces.

Recommended Action Because ICMP is a connectionless protocol, the FWSM does not automatically allow returning traffic through. In addition to an ACL on the source interface, you either need to apply an ACL to destination interface to allow replying traffic, or enable the ICMP inspection engine, which treats ICMP connections as stateful connections.

Symptom Traffic does not go through the FWSM from a higher security interface to a lower security interface.

Possible Cause You did not apply an ACL to the higher security interface to allow traffic through. Unlike the PIX firewall, the FWSM does not automatically allow traffic to pass between interfaces.

Recommended Action Apply an ACL to the source interface to allow traffic through. See the "Adding an Extended Access Control List" section on page 10-13.

Symptom Traffic does not pass between two interfaces on the same security level.

Possible Cause You did not enable the feature that allows traffic to pass between interfaces on the same security level.

Recommended Action Enable this feature according to the "Allowing Communication Between Interfaces on the Same Security Level" section on page 6-8.

Symptom When the FWSM fails over, the secondary unit does not pass traffic.

Possible Cause You did not assign the same VLANs for both units.

Recommended Action Make sure to assign the same VLANs to both units in the switch configuration.