



# CHAPTER 24

## Troubleshooting the Firewall Services Module

---

This chapter describes how to troubleshoot the FWSM, and includes the following sections:

- [Testing Your Configuration, page 24-1](#)
- [Reloading the FWSM, page 24-6](#)
- [Performing Password Recovery, page 24-6](#)
- [Other Troubleshooting Tools, page 24-7](#)
- [Common Problems, page 24-10](#)

### 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 24-5](#).

This section includes:

- [Enabling ICMP Debug Messages and System Log Messages, page 24-1](#)
- [Pinging FWSM Interfaces, page 24-2](#)
- [Pinging Through the FWSM, page 24-4](#)
- [Disabling the Test Configuration, page 24-5](#)

### Enabling ICMP Debug Messages and System Log Messages

Debug messages and system log 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 log messages, perform the following steps:

---

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

```
hostname(config)# debug icmp trace
```

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

```
hostname(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 log messages to your Telnet or SSH session, enter the following command:

```
hostname(config)# terminal monitor
```

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

```
hostname(config)# logging enable
```

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

```
hostname(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 preceding 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.



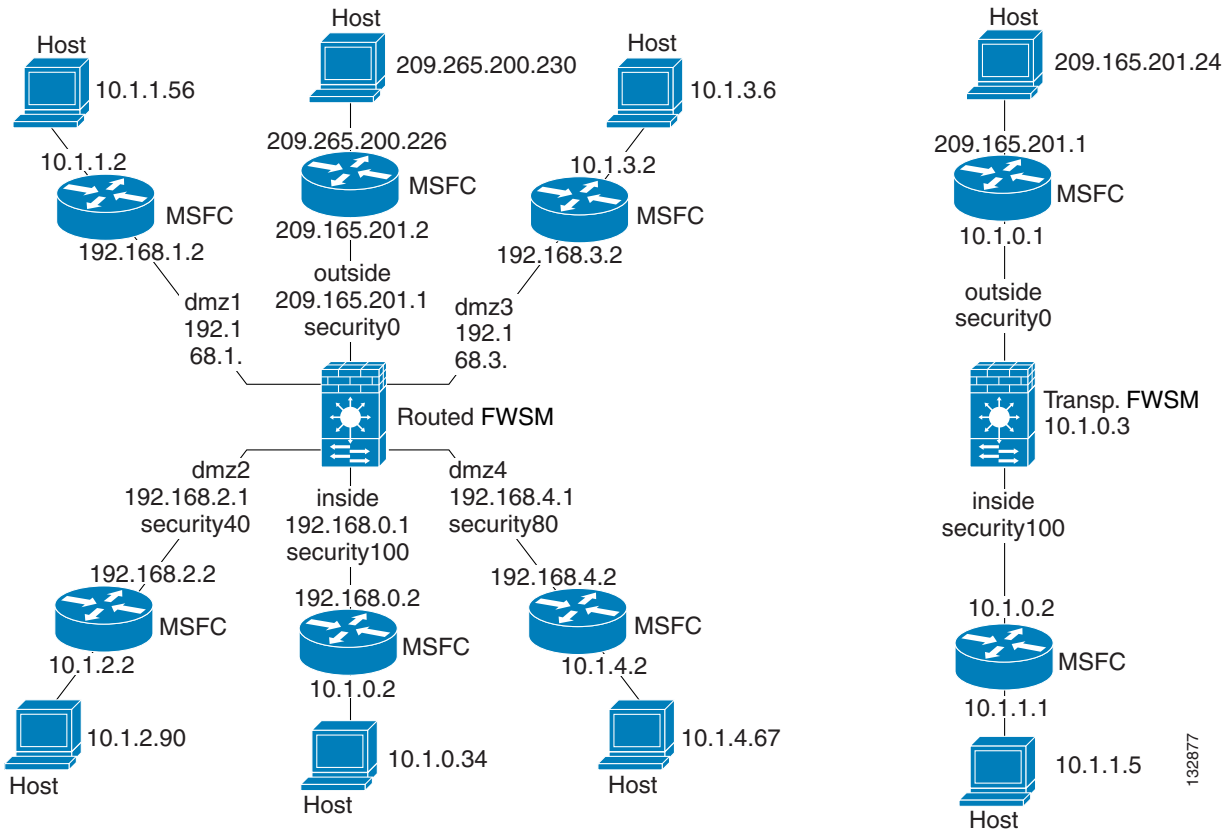
### Note

You can ping only the closest interface. Pinging the far interface is not supported.

To ping the FWSM interfaces, perform the following 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 24-4. For example:

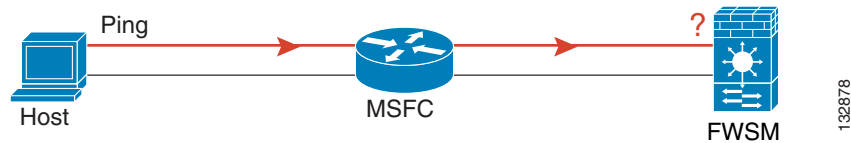
Figure 24-1 Network Sketch with Interfaces, Routers, and Hosts



**Step 2** 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 interface configuration is correct. A ping might fail if the FWSM interface is not active, the interface configuration is incorrect, or if a switch between the FWSM and router is down (see Figure 24-2). In this case, no debug messages or system log messages appear on the FWSM, because the packet never reaches it.

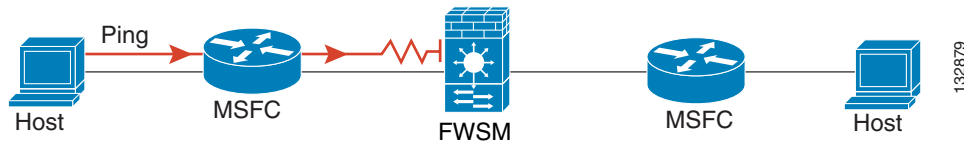
Figure 24-2 Ping Failure at FWSM Interface



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 24-3).

**Figure 24-3 Ping Failure Because of IP Addressing Problems**

- Step 3** 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 24-4). In this case, the debug messages show that the ping was successful, but you see system log message 110001 indicating a routing failure.

**Figure 24-4 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, if configured. 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 Cisco TAC.

To ping between hosts on different interfaces, perform the following steps:

- Step 1** To add an access list allowing ICMP from any source host, enter the following command:

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

By default, when hosts access a lower security interface, all traffic is allowed through. However, to access a higher security interface, you need the preceding access list.

- Step 2** To assign the access list to each source interface, enter the following command:

```
hostname(config)# access-group ICMPACL 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 commands:

```
hostname(config)# class-map ICMP-CLASS
hostname(config-cmap)# match access-list ICMPACL
hostname(config-cmap)# policy-map ICMP-POLICY
hostname(config-pmap)# class ICMP-CLASS
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# service-policy ICMP-POLICY global
```

Alternatively, you can also apply the ICMPACL access list 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 log 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 Cisco TAC.

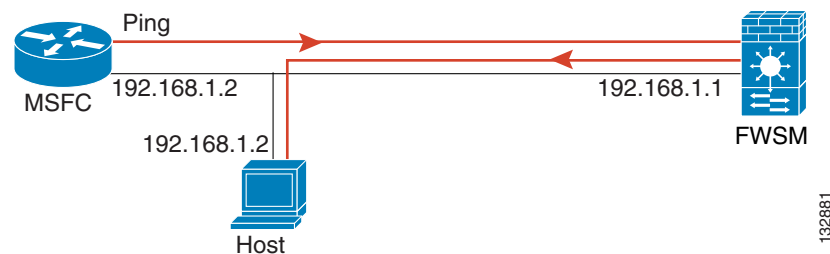
For routed mode, the ping might fail because NAT is not configured correctly (see Figure 24-5). This is more likely if you enable NAT control. In this case, you see a system log message showing that the NAT translation failed (305005 or 305006). If the ping is from an outside host to an inside host, and you do not have a static translation (which is required with NAT control), 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 24-5 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, perform the following steps:

- Step 1** To disable ICMP debug messages, enter the following command:
- ```
hostname(config)# no debug icmp trace
```
- Step 2** To disable logging, if desired, enter the following command:
- ```
hostname(config)# no logging on
```
- Step 3** To remove the ICMPACL access list, and also delete the related **access-group** commands, enter the following command:
- ```
hostname(config)# no access-list ICMPACL
```
- Step 4** (Optional) To disable the ICMP inspection engine, enter the following command:

```
hostname(config)# no service-policy ICMP-POLICY
```

---

## Reloading the FWSM

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

```
hostname# reload
```

## Performing Password Recovery

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, page 24-6](#)
- [Resetting the Maintenance Partition Passwords, page 24-7](#)

## 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 in to the maintenance partition to perform this procedure:

---

**Step 1** Set the application boot partition by entering the following command at the switch prompt:

```
Router# set boot device cf:n [mod_num]
```

The default boot partition for the module is cf:4. The maintenance partition is cf:1. Later in this procedure, you specify the boot partition for which you want to clear passwords.

**Step 2** To boot the FWSM in to the maintenance partition, enter the following command:

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

**Step 3** To session in to the FWSM, enter the following command:

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

**Step 4** To log in to the maintenance partition as root, enter the following command:

```
Login: root
```

**Step 5** Enter the password at the prompt:

```
Password: password
```

By default, the password is “cisco.”

**Step 6** 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}
```

Specify the boot partition for which you want to clear passwords. By default, the FWSM boots from **cf:4**. See [Step 1](#) for more information about viewing the boot partition.

**Step 7** 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.
```

---

## Resetting 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 in to 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:

```
hostname# clear mp-passwd
```

## Other Troubleshooting Tools

The FWSM provides other troubleshooting tools to be used in conjunction with Cisco TAC:

- [Viewing Debug Messages, page 24-7](#)
- [Capturing Packets, page 24-7](#)
- [Viewing the Crash Dump, page 24-9](#)

## Viewing Debug Messages

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use. 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. This section includes the following topics:

- [Capture Overview, page 24-8](#)

- [Capture Limitations, page 24-8](#)
- [Configuring a Packet Capture, page 24-9](#)

## Capture Overview

The FWSM is capable of tracking all IP traffic that flows across it. It is also capable of capturing all the IP traffic that is destined to the FWSM, including all the management traffic (such as SSH and Telnet traffic) to the FWSM.

The FWSM architecture consists of three different sets of processors for packet processing; this architecture poses certain restrictions on the capability of the capture feature. Typically most of the packet forwarding functionality in the FWSM is handled by the two front-end network processors, and packets are sent to the control-plane general-purpose processor only if they need application inspection (see the “[Stateful Inspection Overview](#)” section on page 1-8 for more information). The packets are sent to the session management path network processor only if there is a session miss in the accelerated path processor.

Because all the packets that are forwarded or dropped by the FWSM hits the two front-end network processors, the packet capture feature is implemented in these network processors. So all the packets that hit the FWSM can be captured by these front end processors, if an appropriate capture is configured for those traffic interfaces. On the ingress side, the packets are captured the moment the packet hits the FWSM interfaces, and on the egress side the packets are captured just before they are sent out on the wire.

## Capture Limitations

The following are some of the limitations of the capture feature. Most of the limitations are due to the distributed nature of the FWSM architecture and due to the hardware accelerators that are being used in the FWSM.

- You cannot configure more than one capture per interface. But you can configure multiple ACEs in the capture access list to have a flexible configuration.
- You can only capture IP traffic. Non-IP packets like ARPs cannot be captured by the capture feature.
- For a shared VLAN:
  - You can only configure one capture for the VLAN; if you configure a capture in multiple contexts on the shared VLAN, then only the last capture that was configured is used.

If you remove the last-configured (active) capture, no captures become active, even if you previously configured a capture in another context; you must remove and readd the capture to make it active.

- All traffic that enters the interface to which the capture is attached (and that matches the capture access list) is captured, including traffic to other contexts on the shared VLAN.

Therefore, if you enable a capture in Context A for a VLAN that is also used by Context B, both Context A and Context B ingress traffic is captured.

For egress traffic, only the traffic of the context with the active capture is captured. The only exception is when you do not enable the ICMP inspection (therefore the ICMP traffic does not have a session in the accelerated path). In this case, both ingress and egress ICMP traffic for all contexts on the shared VLAN is captured.

## Configuring a Packet Capture

Configuring a capture typically involves configuring an access list that matches the traffic that needs to be captured. Once an access list that matches the traffic pattern is configured, then you need to define a capture and associate this access list to the capture, along with the interface on which the capture needs to be configured. Note that a capture only works if an access list and an interface are associated with a capture for capturing IPv4 traffic. The access list is not required for IPv6 traffic.

To configure a packet capture for IPv4 traffic, perform the following steps:

- 
- Step 1** Configure an extended access list that matches the traffic that needs to be captured according to the “[Adding an Extended Access List](#)” section on page 10-6.

For example, the following access list identifies all traffic:

```
hostname(config)# access-list capture extended permit ip any any
```

- Step 2** To configure the capture, enter the following command.

```
hostname(config)# capture name access-list acl_name interface interface_name
```

By default configuring a capture creates a linear capture buffer of size 512 KB. You can optionally configure a circular buffer. By default only 68 bytes of the packets are captured in the buffer. You can optionally change this value. See the **capture** command in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for these and other options.

For example, the following command creates a capture called ip-capture using the capture access list configured in [Step 1](#) that is applied to the outside interface:

```
hostname(config)# capture ip-capture access-list capture interface outside
```

- Step 3** To view the capture, enter the following command:

```
hostname(config)# show capture name
```

You can also copy the capture using the **copy capture** command. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information.

- Step 4** To end the capture but retain the buffer, enter the following command:

```
hostname(config)# no capture name access-list acl_name interface interface_name
```

- Step 5** To end the capture and delete the buffer, enter the following command:

```
hostname(config)# no capture name
```

---

## Viewing the Crash Dump

If the FWSM crashes, you can view the crash dump information. We recommend contacting Cisco TAC 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 in to 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 in to 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 7-1 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 4-19.

**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** 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 Access”](#) section on page 21-1 or the [“Allowing SSH Access”](#) section on page 21-2.

**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 21-10.

**Symptom** You cannot ping through the FWSM, even though the access list allows it.

**Possible Cause** You did not enable the ICMP inspection engine or apply access lists 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 access list on the source interface, you either need to apply an access list 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 access list 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 access list to the source interface to allow traffic through. See the [“Adding an Extended Access List”](#) section on page 10-6.

**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 6-5.

**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.

