Configuring the Switch for the Firewall Services Module

This chapter describes how to configure the Catalyst 6500 series switch or the Cisco 7600 series router for use with the Firewall Services Module (FWSM). Before completing the procedures in this chapter, configure the basic properties of your switch, including assigning VLANs to interfaces, according to the documentation that came with your switch.

This chapter includes the following sections:

Switch Overview

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 Multilayer Switch Feature Card (MSFC)).

The switch supports two software modes:

- Cisco IOS software on both the switch supervisor and the integrated MSFC router (known as supervisor IOS).
- Catalyst Operating System (OS) on the supervisor, and Cisco IOS software on the MSFC.

Both modes are described in this guide.

See the "Using the MSFC" section on page 1-9 for more information about the MSFC.

Note For each FWSM in a switch using Cisco IOS software, the SPAN reflector feature is enabled. This feature enables multicast traffic (and other traffic that requires central rewrite engine) to be switched when coming from the FWSM. The SPAN reflector feature uses one SPAN session. To disable this feature, enter the following command:

```
Router(config)# no monitor session servicemodule
```

Verifying the Module Installation

To verify that the switch acknowledges the FWSM and has brought it online, view the module information according to your operating system:

- Cisco IOS Software

```
Router> show module [mod-num | all]
```

The following example shows the output of the **show module** command:

```
Router> show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1     2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
  2    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3     2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4     6  Firewall Module                        WS-SVC-FWM-1       SAD062302U4
```

- Catalyst OS

```
Console> show module [mod-num]
```

The following example shows the output of the **show module** command:

```
Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

Note The **show module** command shows six ports for the FWSM; these are internal ports that are grouped together as an EtherChannel. See the "Customizing the FWSM Internal Interface" section on page 2-11 for more information.

Assigning VLANs to the Firewall Services Module

This section describes how to assign VLANs to the FWSM. The FWSM does not include any external physical interfaces. Instead, it uses VLAN interfaces. Assigning VLANs to the FWSM is similar to assigning a VLAN to a switch port; the FWSM includes an internal interface to the Switch Fabric Module (if present) or the shared bus.

See the following topics:

Prerequisites

Follow these steps to make sure you can use the VLANs on the FWSM. See the documentation for the switch for detailed information.

1. Add the VLANs to the switch.

   If you do not add the VLANs to the switch before you assign them to the FWSM, the VLANs are stored in the supervisor engine database and are sent to the FWSM as soon as they are added to the switch.

   The VLANs cannot be reserved VLANs.

   - **Cisco IOS Software**

     To add the VLAN, enter the **vlan** *vlan_number* command.

   - **Catalyst OS**

     To add the VLAN, enter the **set vlan** *vlan_number* command.

2. Assign the VLANs to switch ports.

   - **Cisco IOS Software**

     To assign a VLAN to a port, enter:

     ```
     router(config)# interface type slot/port
     router(config-if)# switchport
     router(config-if)# switchport mode access
     router(config-if)# switchport access vlan vlan_id
     ```

   - **Catalyst OS**

     To assign a VLAN to a port, enter the **set vlan** *vlan_number mod/ports* command. This command both creates the VLAN (if you have not already done so) and assigns it to a port.

Note If you are using FWSM failover within the same switch chassis, do not assign the VLAN(s) you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.

3. Assign VLANs to the FWSM before you assign them to the MSFC.

   VLANs that do not satisfy this condition are discarded from the range of VLANs that you attempt to assign on the FWSM. See the "Adding Switched Virtual Interfaces to the MSFC" section on page 2-5 for more information.

Assigning VLANs in Cisco IOS Software

In Cisco IOS software, create one or more firewall VLAN groups, and then assign the groups to the FWSM. For example, you can assign all the VLANs to one group, or you can create an inside group and an outside group, or you can create a group for each customer.

You cannot assign the same VLAN to multiple firewall groups; however, you can assign multiple firewall groups to an FWSM. VLANs that you want to assign to multiple FWSMs, for example, can reside in a separate group from VLANs that are unique to each FWSM.

To assign VLANs to the FWSM, follow these steps:

Step 1 To assign VLANs to a firewall group, enter the following command:

```
Router(config)# firewall vlan-group firewall_group vlan_range
```

The *vlan_range* can be one or more VLANs (1 to 1000 and from 1025 to 4094) identified in one of the following ways:

- A single number (*n*)
- A range (*n-x*)

Separate numbers or ranges by commas. For example, enter the following numbers:

```
5,7-10,13,45-100
```

Note Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.

Step 2 To assign the firewall groups to the FWSM, enter the following command:

```
Router(config)# firewall module module_number vlan-group firewall_group
```

The *firewall_group* is one or more group numbers:

- A single number (*n*)
- A range (*n-x*)

Separate numbers or ranges by commas. For example, enter the following numbers:

```
5,7-10
```

This example shows how you can create three firewall VLAN groups: one for each FWSM, and one that includes VLANs assigned to both FWSMs. See the "Prerequisites" section on page 2-3 for more information about adding VLANs to the switch.

```
Router(config)# vlan 55-57,70-85,100
Router(config-vlan)# exit
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

To view the group configuration, enter the following command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

To view VLAN group numbers for all modules, enter the following command:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Assigning VLANs in Catalyst OS Software

In Catalyst OS software, you assign a list of VLANs to the FWSM. You can assign the same VLAN to multiple FWSMs if desired.

To assign VLANs to the FWSM, enter the following command:

```
Console> (enable) set vlan vlan_list firewall-vlan mod_num
```

The *vlan_list* can be one or more VLANs (1 to 1000 and from 1025 to 4094) identified in one of the following ways:

- A single number (*n*)
- A range (*n-x*)

Separate numbers or ranges by commas. For example:

```
5,7-10,13,45-100
```

Note Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.

This example shows a typical configuration:

```
Console> (enable) set vlan 55-57
Console> (enable) set vlan 70-85
Console> (enable) set vlan 100
Console> (enable) set vlan 55-57,100 firewall-vlan 5
Console> (enable) set vlan 70-85,100 firewall-vlan 8
```

To view the VLANs assigned to the FWSM, enter the following command:

```
Console> show vlan firewall-vlan 5
Secured vlans by firewall module 5
55-57, 100
```

Adding Switched Virtual Interfaces to the MSFC

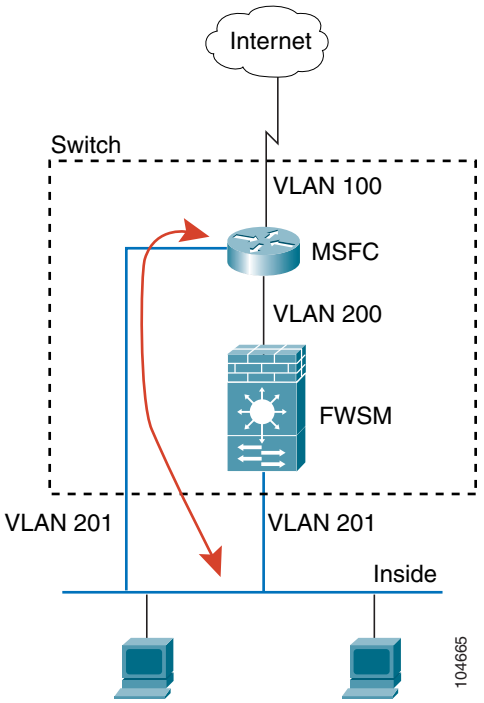
A VLAN defined on the MSFC is called a switched virtual interface (SVI). If you assign the VLAN used for the SVI to the FWSM (see the "Assigning VLANs to the Firewall Services Module" section on page 2-2), then the MSFC routes between the FWSM and other Layer 3 VLANs.

This section includes the following topics:

SVI Overview

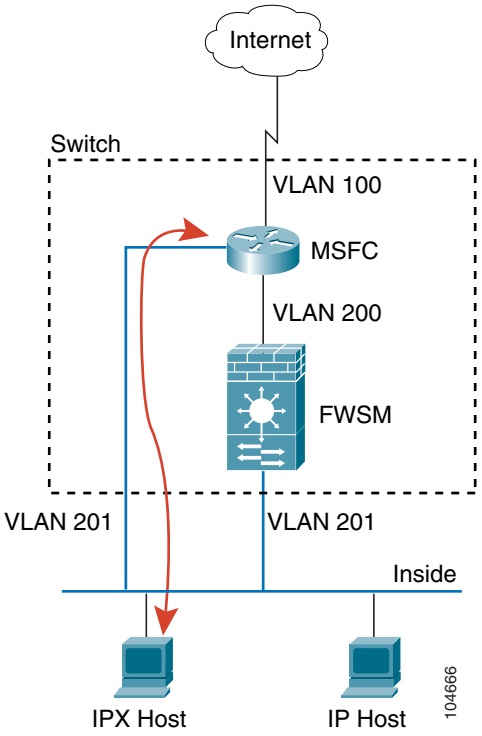
For security reasons, by default, only one SVI can exist between the MSFC and the FWSM. For example, if you misconfigure the system with multiple SVIs, you could accidentally allow traffic to pass around the FWSM by assigning both the inside and outside VLANs to the MSFC (see Figure 2-1).

Figure 2-1 Multiple SVI Misconfiguration



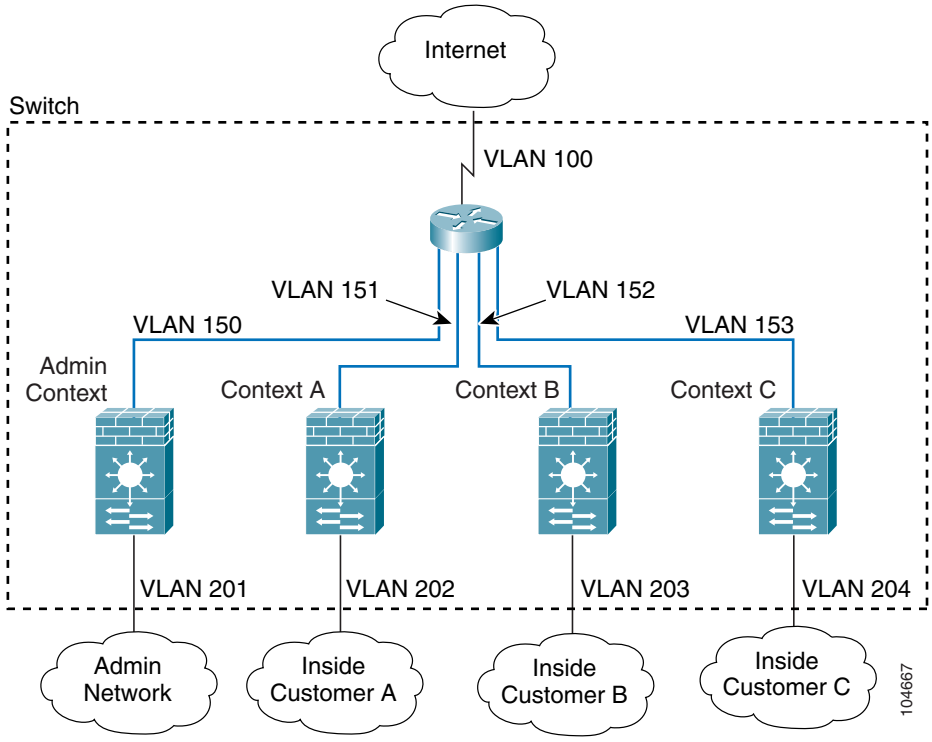
However, you might need to bypass the FWSM in some network scenarios. Figure 2-2 shows an IPX host on the same Ethernet segment as IP hosts. Because the FWSM in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the FWSM for IPX traffic. Make sure to configure the MSFC with an ACL that allows only IPX traffic to pass on VLAN 201.

Figure 2-2 Multiple SVIs for IPX



For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface (see Figure 2-3). You might also choose to use multiple SVIs in routed mode so you do not have to share a single VLAN for the outside interface.

Figure 2-3 Multiple SVIs in Multiple Context Mode



Configuring SVIs for Cisco IOS Software on the Supervisor

If you are running Cisco IOS software on the supervisor, follow these steps to add an SVI to the MSFC:

Step 1 (Optional) To allow you to add more than one SVI to the FWSM, enter the following command:

```
Router(config)# firewall multiple-vlan-interfaces
```

Step 2 To add a VLAN interface to the MSFC, enter the following command:

```
Router(config)# interface vlan vlan_number
```

Step 3 To set the IP address for this interface on the MSFC, enter the following command:

```
Router(config-if)# ip address address mask
```

Step 4 To enable the interface, enter the following command:

```
Router(config-if)# no shut
```

This example shows a typical configuration with multiple SVIs:

```
Router(config)# vlan 55-57,70-85
Router(config-vlan)# exit
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end
Router#
```

To view your SVI configuration, enter the following command:

```
Router# show int vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuring SVIs for Catalyst OS on the Supervisor

If you are running Catalyst OS on the supervisor, follow these steps to add an SVI to the MSFC:

Step 1 (Optional) To allow you to add more than one SVI to the FWSM. enter the following command:

```
Console> (enable) set firewall multiple-vlan-interfaces enable
```

To disable this setting, enter the following command:

```
Console> (enable) set firewall multiple-vlan-interfaces disable
```

Step 2 To access the MSFC interface, enter one of the following commands:

```
Console> (enable) switch console
```

or

```
Console> (enable) session {15 | 16}
```

If you are accessing the switch using Telnet or SSH, you must use the **session** command.

Step 3 To enter enable mode and then configuration mode on the MSFC, enter the following commands:

```
Router> enable
Router# configure terminal
```

Step 4 To add a VLAN interface to the MSFC, enter the following command:

```
Router(config)# interface vlan vlan_number
```

Step 5 To set the IP address for this interface on the MSFC, enter the following command:

```
Router(config-if)# ip address address mask
```

Step 6 To enable the interface, enter the following command:

```
Router(config-if)# no shut
```

Step 7 To return to privileged EXEC mode, enter the following command:

```
Router(config-if)# end
```

Step 8 To return to the switch CLI, enter **Ctrl-C** three times.

This example shows a typical configuration:

```
Console> (enable) set vlan 55-57
Console> (enable) set vlan 70-85
Console> (enable) set vlan 55-57,70-85 firewall-vlan 8
Console> (enable) set firewall multiple-vlan-interfaces enable
Console> (enable) switch console
Router> enable
Password: ******
Router# configure terminal
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end
Router# ^C^C^C
Console> (enable)
```

To view your SVI configuration, enter the following command at the MSFC prompt:

```
Router# show int vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
```

```
Last clearing of "show interface" counters never
Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
Queueing strategy:fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
L3 out Switched:ucast:0 pkt, 0 bytes
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   4 packets output, 256 bytes, 0 underruns
   0 output errors, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

Customizing the FWSM Internal Interface

The connection between the FWSM and the switch is a 6-GB 802.1Q trunking EtherChannel. This EtherChannel is automatically created when you install the FWSM. On the FWSM side, two network processors (NPs) connect to three Gigabit Ethernet interfaces each, and these interfaces comprise the EtherChannel. The switch distributes traffic to the interfaces in the EtherChannel according to a distribution algorithm based on session information; load sharing is not performed on a per-packet basis, but rather on a flow basis. In some cases, the algorithm assigns traffic unevenly between the interfaces and, therefore, between the two NPs. Aside from not utilizing the full processing potential of the FWSM, consistent inequity can result in unexpected behavior when you apply resource management to multiple contexts (see the "Configuring a Class" section on page 5-14 for more information.) To make changes to the algorithm see the command for your operating system:

- Cisco IOS Software

  ```
  Router(config)# port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip |
  src-dst-mac | src-dst-port | src-ip | src-mac | src-port}
  ```

  The default is **src-dst-ip**.

- Catalyst OS

  ```
  Console> (enable) set port channel all distribution {ip | mac | session |
  ip-vlan-session} [source | destination | both]
  ```

  The default is **ip both**.

Configuring the Switch for Failover

To configure the switch for failover, see the following topics:

- Assigning VLANs to the Secondary Firewall Services Module, page 2-12
- Adding a Trunk Between a Primary Switch and Secondary Switch, page 2-12
- Ensuring Compatibility with Transparent Firewall Mode, page 2-12

Assigning VLANs to the Secondary Firewall Services Module

Because both units require the same access to the inside and outside networks, you must assign the same VLANs to both FWSMs on the switch(es). See the "Assigning VLANs to the Firewall Services Module" section on page 2-2.

Adding a Trunk Between a Primary Switch and Secondary Switch

If you are using inter-switch failover (see the "Module Placement" section on page 15-4), then you need to configure an 802.1Q VLAN trunk between the two switches. The trunk should have the following characteristics:

- The trunk must carry all firewall VLANs, including the failover and state VLANs.
- Because this trunk also accommodates FWSM traffic when a module fails, this trunk should be at least as large as the maximum amount of traffic you expect to be inspected by the FWSM. The FWSM has an internal 6-Gbps EtherChannel to the switch, so if the FWSM runs at full capacity, the trunk between the two devices needs to include at least six 1-Gbps interfaces. EtherChannel aggregates the bandwidth of up to eight compatibly configured ports into a single logical link. If you do not have the ports to spare, you can create a smaller trunk; however, you might experience decreased performance.
- The trunk should have QoS enabled so that failover VLAN packets, which have the COS value of 5 (higher priority), are treated with higher priority in these ports.

To configure the EtherChannel and trunk, see the documentation for your switch.

Ensuring Compatibility with Transparent Firewall Mode

To avoid loops when you use failover in transparent mode, use switch software that supports BPDU forwarding. Catalyst OS Version 8.2(1) and Cisco IOS Version 12.2(17)SXA allow BPDUs automatically.

Managing the Firewall Services Module Boot Partitions

This section describes how to reset the FWSM from the switch, and how to manage the boot partitions on the Compact Flash card. This section includes the following topics:

Flash Memory Overview

The FWSM has a 128-MB Compact Flash card ("Flash memory") that stores the operating system, configurations, and other data. The Flash memory includes six partitions, called **cf:***n* in Cisco IOS and Catalyst operating system commands:

- Maintenance partition (**cf:1**)—Contains the maintenance image. Use the maintenance partition to upgrade or install application images if you cannot boot into the application partition, to reset the application image password, or to display the crash dump information.
- Network configuration partition (**cf:2**)—Contains the network configuration of the maintenance image. The maintenance partition requires IP settings so that the FWSM can reach the TFTP server to download software images.
- Crash dump partition (**cf:3**)—Stores the crash dump information.
- Application partitions (**cf:4** and **cf:5**)—Stores the software image, system configuration, and PDM for FWSM. By default, Cisco installs the images on **cf:4**. You can use **cf:5** as a test partition. For example, if you want to upgrade your software, you can install the new software on **cf:5**, but maintain the old software as a backup in case you have problems.
- Security context partition (**cf:6**)—64 MB are dedicated to this partition, which stores security context configurations (if desired) and RSA keys in a navigable file system. All other partitions do not have file systems that allow you to perform common tasks such as listing files. This partition is called **disk** when using the **copy** command.

Setting the Default Boot Partition

By default, the FWSM boots from the **cf:4** application partition. However, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. To change the default boot partition, enter the command for your operating system:

- Cisco IOS Software

  ```
  Router(config)# boot device module mod_num cf:n
  ```

  Where *n* is 1 (maintenance), 4 (application), or 5 (application).

- Catalyst OS

  ```
  Console> (enable) set boot device cf:n mod_num
  ```

  Where *n* is 1 (maintenance), 4 (application), or 5 (application).

Resetting the FWSM or Booting from a Specific Partition

This section describes how to reset the FWSM or boot from a specific partition. You might need to reset the FWSM if you cannot reach it through the CLI or an external Telnet session. You might need to boot from a non-default boot partition if you need to access the maintenance partition or if you want to boot from a different software image in the backup application partition. The maintenance partition is valuable for troubleshooting.

The reset process might take several minutes.

For Cisco IOS software, when you reset the FWSM, you can also choose to run a full memory test. When the FWSM initially boots, it only runs a partial memory test. A full memory test takes approximately 6 minutes.

To reset the FWSM, see the section for your operating system:

- Resetting the FWSM in Cisco IOS Software, page 2-14
- Resetting the FWSM in Catalyst OS, page 2-14

Note To reload the FWSM when you are logged into the FWSM, enter **reload** or **reboot**. You cannot boot from a non-default boot partition with these commands.

Resetting the FWSM in Cisco IOS Software

To reset the FWSM from the switch CLI, enter the following command:

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

The **cf:***n* argument is the partition, either 1 (maintenance), 4 (application), or 5 (application). If you do not specify the partition, the default partition is used (typically **cf:4**).

The **mem-test-full** option runs a full memory test, which takes approximately 6 minutes.

This example shows how to reset the FWSM installed in slot 9. The default boot partition is used.

```
Router# hw-mod mod 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

Resetting the FWSM in Catalyst OS

To reset the FWSM from the switch CLI, enter the following command:

```
Console> (enable) reset mod_num [cf:n]
```

where **cf:***n* is the partition, either 1 (maintenance), 4 (application), or 5 (application). If you do not specify the partition, the default partition is used (typically cf:4).