



# CHAPTER 4

## Configuring the Switch for Use with the FWSM

---

This chapter describes how to configure the Catalyst 6500 series switch or the Cisco 7600 series router for use with the FWSM. This chapter includes some functions that you must configure using the switch CLI; other procedures can be completed using ASDM.

This chapter includes the following sections:

- [Switch Overview, page 4-1](#)
- [Verifying the Module Installation at the CLI, page 4-3](#)
- [Configuring the Switch to Support ASDM, page 4-3](#)
- [Establishing Connectivity with the Switch, page 4-4](#)
- [Configuring Switch Ports, page 4-4](#)
- [Configuring VLANs and Switched Virtual Interfaces, page 4-7](#)
- [Configuring Firewall VLAN Groups, page 4-11](#)
- [Customizing the FWSM Internal Interface at the CLI, page 4-14](#)
- [Configuring the Switch for Failover, page 4-14](#)
- [Managing the Firewall Services Module Boot Partitions at the CLI, page 4-15](#)

### Switch Overview

This section describes ASDM support of the switch, and includes the following topics:

- [Supported Switch Configuration Using ASDM, page 4-1](#)
- [Supported Switch Hardware and Software, page 4-2](#)
- [Configuring the Switch in Multiple Context Mode, page 4-2](#)

### Supported Switch Configuration Using ASDM

Using ASDM, you can configure the following switch functions:

- Assign ports to a VLAN.
- Configure port parameters such as the admin status, speed and PortFast.
- Set the port mode to routed or switched.
- Configure VLANs.

- Configure SVIs
- Configure firewall VLAN groups and assign them to the FWSM

**Note**

The following functions are not supported in the Configuration > Switch pane in ASDM:

- Trunk port configuration
- VLAN groups for intra-chassis Active/Active failover
- VLAN groups for inter-chassis failover

## Supported Switch Hardware and Software

You can install the FWSM in the Catalyst 6500 series switches or the Cisco 7600 series routers. The configuration of both series is identical, and the series are referred to generically in this guide as the “switch.” The switch includes a switch (the supervisor engine) as well as a router (the MSFC).

The switch supports Cisco IOS software on both the switch supervisor engine and the integrated MSFC router.

**Note**

The Catalyst operating system software is not supported.

The FWSM runs its own operating system.

See the [“Using the MSFC” section on page 1-15](#) for more information about the MSFC.

Some FWSM features interact with Cisco IOS features, and require specific Cisco IOS software versions. See the [“Switch Hardware and Software Compatibility” section on page A-2](#) for more information. The following features involve Cisco IOS software, and are described in the feature sections:

- Route Health Injection—See the [“Configuring Route Health Injection” section on page 10-45](#).
- PISA integration—See the [“Using PISA to Permit or Deny Application Types” section on page 26-5](#).
- Virtual Switching System (VSS) support—No FWSM configuration required.

**Note**

For Cisco IOS software Version 12.2(18)SX6 and earlier, for each FWSM in a switch, 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
```

## Configuring the Switch in Multiple Context Mode

In multiple context mode, you can configure the switch using ASDM only if you connect to the admin context. If you connect to ASDM in a non-admin context, you cannot access the switch configuration.

## Verifying the Module Installation at the CLI

To verify that the switch acknowledges the FWSM and has brought it online, view the module information by entering the following command:

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

The following is sample output from 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
```



### 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 at the CLI”](#) section on page 4-14 for more information.

## Configuring the Switch to Support ASDM

Before you can use ASDM to configure the switch, you need to configure SNMP and SSH settings on the switch using the CLI. To configure the switch, perform the following steps:

**Step 1** Configure the SNMP community using the following command:

```
Router(config)# snmp-server community string
```

Where the *string* argument is a community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

See the Cisco IOS command reference for information about other options in this command.

**Step 2** To enable SSH, enter the following commands:

```
Router(config)# hostname hostname
Router(config)# ip domain-name domain-name
Router(config)# crypto key generate rsa usage-keys modulus 1024
Router(config)# line vty line-number [ending-line-number]
Router(config)# transport input ssh
Router(config)# ip ssh time-out 120
```

See the Cisco IOS command reference for information about these commands.

**Step 3** Be sure to configure a username and password for the ASDM user when they connect to the switch using ASDM, using the **login local**, **login tacacs**, or **login authentication** command. See the Cisco IOS user documentation for more information about user accounts.

## Establishing Connectivity with the Switch

When you connect to the switch in ASDM, you are prompted for SNMP and SSH credentials. Every time you restart ASDM, you need to reenter your credentials; only the switch IP address and SSH username are remembered.

For switch configuration prerequisites, see the [“Configuring the Switch to Support ASDM” section on page 4-3](#).

To establish connectivity with the switch, perform the following steps:

---

**Step 1** Click **Configuration** and then **Switch**.

The Switch Credentials dialog box appears.

**Step 2** In the Sup IP Address field, enter the management IP address of the switch supervisor engine.

**Step 3** In the SNMP Credentials > Read Community field, enter the SNMP community string that you configured in the [“Configuring the Switch to Support ASDM” section on page 4-3](#).

**Step 4** In the SSH Credentials area, enter the following values:

- User Name
- Password
- Enable Password

**Step 5** Click **OK**.

ASDM connects to the switch and loads the switch interface and VLAN information.

If ASDM fails to connect to the switch, click off of the Switch button, and then click the **Switch** button again to access the Switch Credentials dialog box again.

---



**Note**

If you click the **Refresh** button, ASDM refreshes the FWSM configuration first, and then the switch configuration. In multiple mode, it refreshes the currently selected configuration (system or context), and then the switch configuration. There is no separate Refresh button for the switch alone.

---

## Configuring Switch Ports

ASDM lets you configure port parameters and also lets you assign switch ports to VLANs. This section includes the following topics:

- [Using the Interfaces Pane, page 4-5](#)
- [Configuring Port Parameters, page 4-5](#)
- [Assigning Ports to a VLAN, page 4-6](#)

## Using the Interfaces Pane

The Configuration > Switch > Interfaces pane lets you set port parameters and assign switch ports to VLANs, but it also lets you set many other parameters for an easy configuration flow. You can use the Configuration > Switch > Interfaces pane for switch configuration tasks that are also configurable using the Vlans and Vlan Groups panes, as well as FWSM configuration that is available using the Configuration > Interfaces and Configuration > Security Contexts panes. These duplicate functions include:

- Setting a VLAN as a switch virtual interface (SVI) and assigning an IP address and mask (Vlans pane)
- Assigning a VLAN to a VLAN group (Vlan Groups pane)
- Setting the FWSM interface parameters (Configuration > Interfaces pane)

Many essential items are not included on the Interfaces pane, so be sure to check the other panes for additional configuration. For example, you can add a VLAN group from the VLAN groups pane, but not from the Interfaces pane.

In multiple context mode, the Interfaces pane changes depending on whether you are in the system, the admin context, or in another context (remember that to use the Configuration > Switch panes, you must initially connect to the admin context. After you connect, you can change your view to the system or any other context).

In the system, you can view all context VLAN assignments. Within each context, you can only view whether a VLAN is assigned to the current context.

**Note**

The internal EtherChannels of 6 ports each that connect the switch to each FWSM are listed in the Interfaces pane; however, you cannot configure these ports in ASDM.

## Configuring Port Parameters

Port parameters include the speed, administrative state (up or down), PortFast setting, and the mode (routed or switchport).

To configure switch port parameters, perform the following steps:

- 
- Step 1** From the Configuration > Switch > Interfaces pane, click the port you want to configure. You can either edit the settings directly in the table by clicking the cell you want to edit, or you can click **Modify Port(s) Parameters**.
- Step 2** Set the following parameters:
- Speed(Mb/s)—Choose the appropriate value from the drop-down list.
  - Admin St—Choose Up or Down from the drop-down list.
  - Port Fast—Check the box to enable STP PortFast for ports in switchport mode. STP PortFast causes a Layer 2 LAN port configured as an access port to enter the forwarding state immediately, bypassing the listening and learning states. You can use PortFast on Layer 2 access ports connected to a single workstation or server to allow those devices to connect to the network immediately, instead of waiting for STP to converge. Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). When configured for PortFast, a port is still running the spanning tree protocol. A PortFast enabled port can immediately transition to the blocking state if necessary (this could happen on receipt of a superior BPDU).

- Mode—Set the mode to Switchport access mode, or to Routed mode.



**Note** ASDM lets you assign Routed mode to a port; however, because you cannot assign a routed port to a VLAN, you cannot use that port with the FWSM.

**Step 3** If you set the mode to Routed, you can then configure the switch IP address and mask by double-clicking the **Switch IP Add** and **Mask** cells and typing in a value.

In multiple context mode, if you set the IP address within a context, then ASDM makes sure the IP address is not a duplicate of one in the context when you apply the configuration. If you set the IP address in the system, then no checks are performed.

**Step 4** Click **Apply** to apply your changes, or continue on to [“Assigning Ports to a VLAN” section on page 4-6](#) for ports in switchport mode.

## Assigning Ports to a VLAN

You can assign ports in Switchport mode to a VLAN. To assign ports to a VLAN, perform the following steps:

**Step 1** From the Configuration > Switch > Interfaces pane, click one or more ports (in Switchport mode) that you want to assign to the same VLAN. To select discontinuous ports, Ctrl+click the ports. To select contiguous ports, Shift+click the ports.



**Note** If you are using FWSM intra-chassis failover, do not assign a switch port to the VLAN(s) you are reserving for failover and stateful communications.

**Step 2** Click **Assign Port(s) to Vlan**.

The Assign Ports to Vlan dialog box appears.

**Step 3** Choose a VLAN ID in the Vlan# drop-down list, or add a new VLAN by clicking **Add**.

For information about adding a VLAN, see the [“Configuring VLANs and Switched Virtual Interfaces” section on page 4-7](#).

If you selected a single port, you can alternatively set the VLAN directly in the table by clicking the Vlan Id cell and selecting a VLAN from the drop-down list.

**Step 4** Click **OK**.

**Step 5** (Optional) To assign the VLAN to an existing VLAN group, use one of the following options:

- Assign the VLAN to a VLAN group that is assigned to an FWSM—(A VLAN that is in a VLAN group assigned to an FWSM is known as a *secured VLAN*.) Check **Secured**, and then click the **VlanGroup** cell and choose a VLAN group ID from the drop-down menu. Only VLAN groups that are assigned to an FWSM are listed. By default in multiple context mode, the VLAN is assigned to the current context. If you are in the system, then the VLAN is not assigned to any context.
- Assign the VLAN to a VLAN group that is not yet assigned to an FWSM—Click the **VlanGroup** cell and choose a VLAN group ID from the drop-down menu; do not click **Secured**. Only VLAN groups that are not yet assigned to an FWSM are listed.

For more information about adding and configuring VLAN groups, see the “[Configuring Firewall VLAN Groups](#)” section on page 4-11.

- Step 6** (Optional) For a secured VLAN, you can set the FWSM interface name, security level, IP address, and mask by double-clicking the cells in the table and typing in a value. (If the FWSM is in transparent mode, you can set the interface name and security level only). In multiple context mode, you can only edit these fields when the VLAN is assigned to the current context. You cannot edit these settings in the system.

For more information about FWSM interface settings, see [Chapter 8, “Configuring Interfaces.”](#)

- Step 7** (Optional) To create an SVI for a VLAN, configure the switch IP address and mask by double-clicking the **Switch IP Add** and **Mask** cells and typing in a value.

If you want to add more than one SVI, be sure to enable that function on the Vlans pane. For more information about SVIs, see the “[Configuring VLANs and Switched Virtual Interfaces](#)” section on page 4-7.

In multiple context mode, if you set the IP address within a context, then ASDM makes sure the IP address is not a duplicate of one in the context when you apply the configuration. If you set the IP address in the system, then no checks are performed.

- Step 8** Click **Apply**.



**Note** If a VLAN does not exist in Configuration > Switch > Vlans but you assign it to a port, then the Vlan Name, Secured, Vlan Group, Switch IPAdd, and Mask options cannot be modified.

In multiple context mode, if you allocate a new VLAN to a security context, then you need to refresh the system configuration.

## Configuring VLANs and Switched Virtual Interfaces

ASDM lets you add VLANs to the supervisor and also lets you set which of those VLANs are switch virtual interfaces (SVIs) on the MSFC. If you assign the VLAN used for the SVI to the FWSM (see the “[Configuring Firewall VLAN Groups](#)” section on page 4-11), then the MSFC routes between the FWSM and other Layer 3 VLANs.

This section includes the following topics:

- [VLAN Guidelines, page 4-7](#)
- [SVI Overview, page 4-8](#)
- [Configuring VLANs and SVIs, page 4-10](#)

### VLAN Guidelines

See the following guidelines for using VLANs with the FWSM:

- You can use private VLANs with the FWSM. Assign the primary VLAN to the FWSM; the FWSM automatically handles secondary VLAN traffic.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.

- Use VLAN IDs 2 to 1000 and from 1025 to 4094.

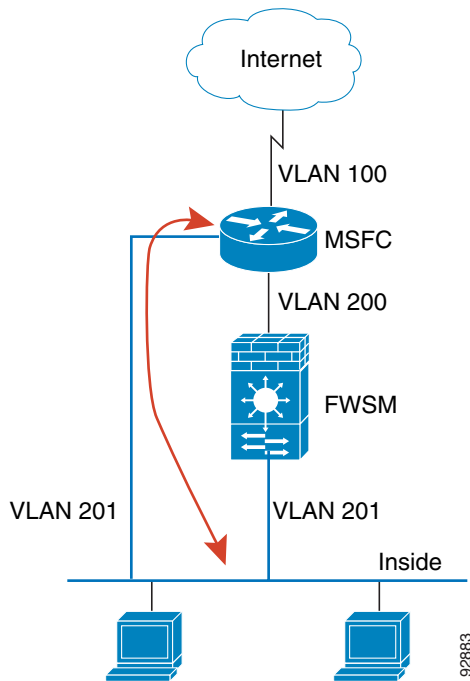
**Note**

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

## 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 4-1](#).)

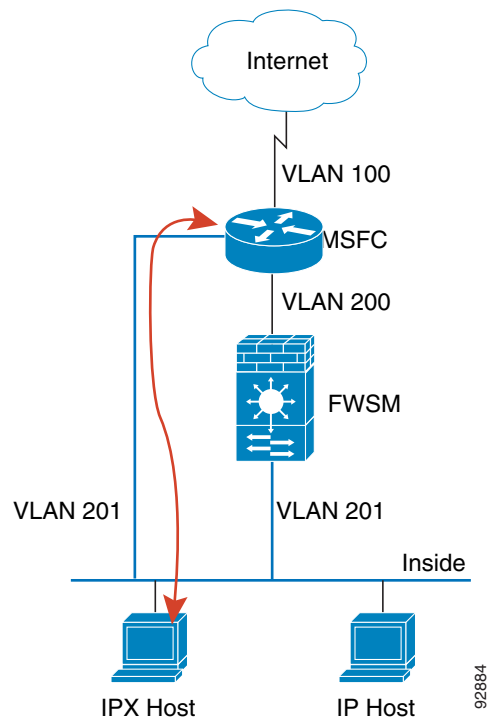
**Figure 4-1** Multiple SVI Misconfiguration



92883

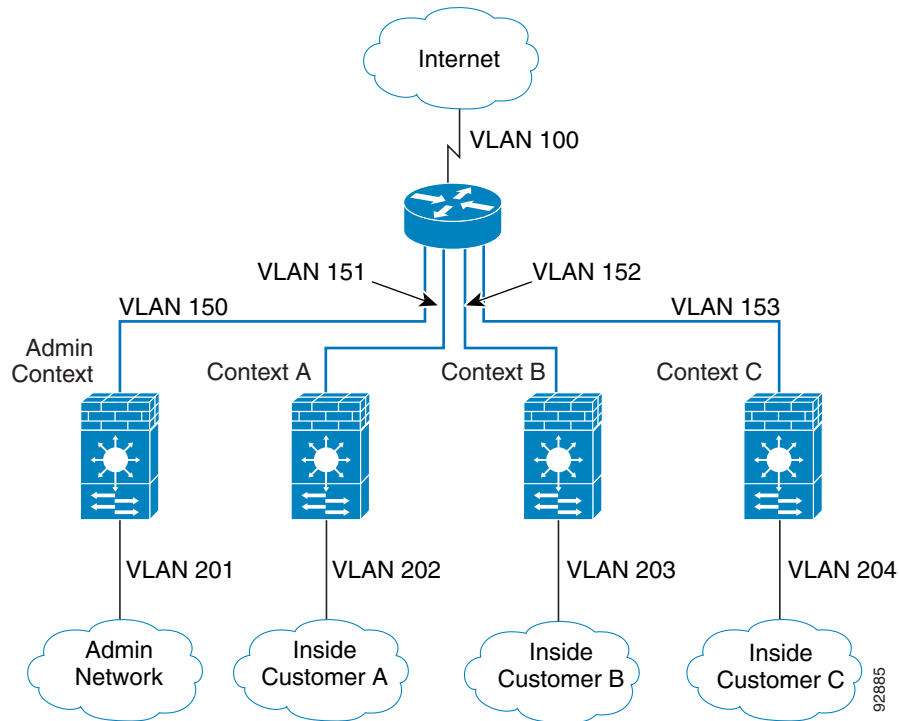
However, you might need to bypass the FWSM in some network scenarios. [Figure 4-2](#) shows an IPX host on the same Ethernet segment as IP hosts. Because the FWSM in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the FWSM for IPX traffic. Make sure to configure the MSFC with an access list that allows only IPX traffic to pass on VLAN 201.

**Figure 4-2** 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 4-3](#)). 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 4-3 Multiple SVIs in Multiple Context Mode**



## Configuring VLANs and SVIs

Perform the following steps to configure VLANs and SVIs:

- 
- Step 1** (Optional) Go to the Configuration > Switch > Vlans pane.
- Step 2** To allow you to add more than one SVI to the FWSM, check **Allow to add more than one SVI to FWSM**.
- Step 3** To add a VLAN, click **Add**.  
The Add Vlan dialog box appears.
- Step 4** You can add a single VLAN or a range of VLANs:
- To add a single VLAN, click **Add single VLAN** and enter the following values:
    - Vlan Id—Enter a VLAN ID. See the “[VLAN Guidelines](#)” section on page 4-7 for more information about VLANs you can use with the FWSM.
    - (Optional) Vlan Name—Enter a name for the VLAN. By default, the name is `VLANnumber`.
    - (Optional) SVI—If you want to make this VLAN an SVI, check **SVI**.  
Switch Interface IP—Enter the IP address for the SVI.

Switch Interface Mask—Enter the mask.

- To add a range of VLANs, click **Add VLAN Range** and enter a range of VLAN IDs separated by commas and/or dashes. For example, 2-5,7,10-20.

After you add the VLAN range, you can configure individual attributes in the VLANs table.

**Step 5** Click **OK**.

The VLANs are added to the Vlans table.

**Step 6** (Optional) In the Vlans table, you can do inline editing for the following:

- Change the VLAN name.

A VLAN name is not editable in the following cases: for VLANs 2 to 1001, when the switch is in VTP client mode; when the VLAN ID is 1, or 1002 to 1005.

- Enable or disable SVI by checking **SVI**.

Be sure to enable multiple SVIs (see [Step 2](#)) to enable this setting for multiple VLANs; however, even if the multiple SVI feature is disabled, you can enable the SVI state for multiple VLANs if they are not secured VLANs (assigned to an FWSM). The SVI state is not editable for VLAN 1.

- Change the SVI IP address and mask (if SVI is enabled).
- Assign the VLAN to a VLAN group. See the next step for more information.




---

**Note** The Secured and Vlan Groups fields are not editable.

---

**Step 7** To delete a VLAN, select the VLAN row in the table, and click **Delete**.

This action also deletes the SVI corresponding to that VLAN, and deletes the VLAN from the VLAN group if it is assigned.

**Step 8** Click **Apply**.




---

**Note** Private VLAN configuration on the switch is not supported using ASDM.

---

## Configuring Firewall VLAN Groups

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.

This section includes the following topics:

- [VLAN Group Guidelines, page 4-11](#)
- [Configuring a VLAN Group and Assigning it to the FWSM, page 4-12](#)

### VLAN Group Guidelines

See the following guidelines for VLAN groups:

- You can assign up to 16 firewall VLAN groups to each 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.
- Each group can contain multiple VLANs.
- You cannot assign the same VLAN to multiple VLAN groups; however, you can assign multiple VLAN groups to an FWSM and you can assign a single VLAN group to multiple FWSMs. 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.




---

**Note** ASDM only lets you assign VLAN groups to the current FWSM and its standby unit; however, you can open another ASDM session to a different FWSM on the same switch and see the same VLAN groups for assignment, so you can share VLAN groups between FWSMs.

---

- For intra-chassis failover, ASDM lets you automatically assign the same VLAN groups to the secondary unit.




---

**Note** If you enable failover after you assign VLAN groups to an FWSM, then ASDM does not support adding the groups to the standby unit; similarly, if you later disable failover, ASDM does not support removing VLAN groups from a standby unit. You need to use the CLI to make these changes. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for more information.

---

- For inter-chassis failover, you need to assign the same VLANs to the secondary unit separately. You must also include the VLANs in the trunk port between the chassis. See the [“Configuring the Switch for Failover” section on page 4-14](#) for more information.

## Configuring a VLAN Group and Assigning it to the FWSM

To create a VLAN group and assign it to the FWSM, perform the following steps:

- 
- Step 1** From the Configuration > Switch > Vlan Groups pane, to add or edit a selected VLAN group, click **Add** or **Edit**.
- The Add/Edit Firewall Vlan Group dialog box displays.
- Step 2** In the Vlan Group area, enter the VLAN group ID as an integer in the Firewall vlan group field.
- Step 3** Choose one or more VLAN IDs in the left table and click the >> button to add them to the group. To remove a VLAN, choose it in the right table and click the << button.
- Step 4** To assign the VLAN group to the current FWSM, click **Assign vlan group to current FW module**. By default in multiple context mode, the VLANs in the group are assigned to the current context. If you are in the system, you can select the contexts to which to assign the VLANs (see [Step 6](#)). For more information about assigning VLANs to contexts, see the [“Configuring Security Contexts” section on page 9-22](#).
- Step 5** If you have intra-chassis failover enabled, enter the module slot number for the standby unit in the Standby module slot field.

The same VLAN group must be assigned to both failover units. For inter-module failover, you have to assign the VLANs to the standby unit separately. See the [“Verifying the Module Installation at the CLI” section on page 4-3](#) to view the FWSM slots.



**Note** If you enable failover after you assign VLAN groups to an FWSM, then ASDM does not support adding the groups to the standby unit; similarly, if you later disable failover, ASDM does not support removing VLAN groups from a standby unit. You need to use the CLI to make these changes. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for more information.

**Step 6** (Optional) If you assigned the VLAN group to the current FWSM, then you can configure FWSM interface settings, and for multiple context mode, context settings.

For more information about configuring Interface settings, see [Chapter 8, “Configuring Interfaces.”](#) For more information about assigning VLANs to contexts, see the [“Configuring Security Contexts” section on page 9-22](#).

You can later edit the settings in the Configuration > Switch > Interfaces table; you cannot edit settings in the Vlan Groups area after you apply them.

- a. In the Firewall Configuration area, in the FW Interface Name field, enter an interface name.  
If you have only one VLAN in the group, the name is used as-is. But if you have multiple VLANs in the group, the name is appended with the VLAN ID. For example, if you enter inside for the name, and the group includes VLANs 2, 3, and 4, then the names will be inside2, inside3, and inside4.
- b. In the Security Level field, enter the security level between 0 and 100.
- c. In the FW Interface IP field, enter the IP address. This field is only available if you have one VLAN in the group because you cannot assign the same IP address to multiple interfaces. In the system, if a group with a single VLAN is assigned to multiple contexts, you cannot assign the IP address because a shared VLAN cannot have the same IP address in multiple contexts.
- d. In the FW Interface Mask field, enter the subnet mask. This field is only available if you have one VLAN in the group. In the system, if a group with a single VLAN is assigned to multiple contexts, then you cannot configure the mask.
- e. In multiple context mode, in the system, set the contexts to which you want to assign the VLAN group by choosing one or more context names in the left table and clicking the >> button.

To add a new context, click **Add**. You need to set the context name and the URL for its configuration file.

To remove a context, select it in the right table, and click the << button.

If you are within a context, the current context is selected and is not configurable. If you want to later assign the same VLANs to another context, you can change to the other context and edit the group in the Vlan Groups pane. Any interface settings you set are assigned to the new current context.

If you choose multiple contexts, then the interface settings you set are inherited by each context.



**Note** If you add VLANs to a VLAN group that is already assigned to an FWSM, then the Firewall Configuration area only applies to the newly added VLANs.

**Step 7** Click **OK**.

**Step 8** On the Vlan Groups pane, click **Apply**.

---

## Customizing the FWSM Internal Interface at the CLI

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 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.

```
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**.

## Configuring the Switch for Failover

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

- [Adding a Trunk Between a Primary Switch and Secondary Switch, page 4-14](#)
- [Ensuring Compatibility with Transparent Firewall Mode, page 4-14](#)
- [Enabling Autostate Messaging for Rapid Link Failure Detection, page 4-15](#)

## Adding a Trunk Between a Primary Switch and Secondary Switch

If you are using inter-switch failover, then you should configure an 802.1Q VLAN trunk between the two switches to carry the failover and state links. 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. See the [“Switch Hardware and Software Compatibility” section on page A-2](#) for more information about switch support for transparent firewall mode.

Do not enable LoopGuard globally on the switch if the FWSM is in transparent mode. LoopGuard is automatically applied to the internal EtherChannel between the switch and the FWSM, so after a failover and a fallback, LoopGuard causes the secondary unit to be disconnected because the EtherChannel goes into the err-disable state.

## Enabling Autostate Messaging for Rapid Link Failure Detection

Using Catalyst operating system software Release 8.4(1) and higher or Cisco IOS software Release 12.2(18)SXF5 and higher, the supervisor engine can send autostate messages to the FWSM about the status of physical interfaces associated with FWSM VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the FWSM that the VLAN is down. This information lets the FWSM declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the FWSM takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

The switch supervisor sends an autostate message to the FWSM when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

**Note**

The switch supports autostate messaging only if you install a single FWSM in the chassis.

In Cisco IOS software, autostate messaging is disabled by default. To enable autostate messaging in Cisco IOS software, enter the following command:

```
Router(config)# firewall autostate
```

The Catalyst operating system software has autostate messaging enabled by default, and it is not configurable. However, autostate in the Catalyst operating system is only available for SVIs. If you want to take advantage of this feature, you can create “dummy” SVIs for all VLANs; simply do not configure any IP addresses for them. For example, the following configuration enables multiple SVIs, and then creates SVIs for VLANs 55 and 56, but does not assign any IP addresses to them:

```
Console> (enable) set vlan 55-56 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)# interface vlan 56  
Router(config-if)# end  
Router# ^C^C^C  
Console> (enable)
```

## Managing the Firewall Services Module Boot Partitions at the CLI

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

- [Flash Memory Overview, page 4-16](#)
- [Setting the Default Boot Partition, page 4-16](#)
- [Resetting the FWSM or Booting from a Specific Partition, page 4-17](#)

## Flash Memory Overview

The FWSM has a 128-MB Flash memory card 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 software commands:

- Maintenance partition (**cf:1**)—Contains the maintenance software. Use the maintenance software 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 software. The maintenance software requires IP settings so that the FWSM can reach the TFTP server to download application software images.
- Crash dump partition (**cf:3**)—Stores the crash dump information.
- Application partitions (**cf:4** and **cf:5**)—Stores the application software image, system configuration, and ASDM. 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. Each partition includes its own startup configuration.
- 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. 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. Each application partition has its own startup configuration.

To change the default boot partition, enter the following command:

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

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

To view the current boot partition, enter the following command:

```
Router# show boot device [mod_num]
```

For example:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

## 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.

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 six minutes.

**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.

To reset the FWSM, 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-module module 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 ...
```

