



## Getting Started

---

This chapter describes how to begin configuring the Firewall Services Module from the CLI and contains these sections:

- [Configuration Overview, page 3-1](#)
- [Saving the Configuration, page 3-8](#)
- [Using PDM, page 3-8](#)

## Configuration Overview

This section describes the Firewall Services Module configuration and contains these sections:

- [Configuring the Switch Interface, page 3-3](#)
- [Sessioning into the Module, page 3-5](#)
- [Configuring the Module, page 3-7](#)

The Firewall Services Module can be used in a variety of topologies depending on the needs of your network. For example, in a data center you may want to provide access control or segregate your security domains. The security domain can be a collection of servers with the same security level. Within that domain, multiple subnets or server farms can exist.

When you configure the Firewall Services Module to function on the perimeter of the network, the module can provide access control to the inside network as a whole, or segregate multiple security zones through VLAN interfaces of different security levels. The security zones can be either in the same network or can define the boundaries of multiple customer networks.

You can configure secure VLANs with both the Cisco IOS and Catalyst operating system software. The secure VLAN information is passed from the switch operating system software to the firewall module when it boots up and comes online. The module accepts traffic on the secure VLANs only after the firewall interfaces are configured on the module corresponding to the secure VLANs defined on the switch. The firewall software should not receive traffic on VLANs unknown to the firewall module or on the secure VLANs without having corresponding firewall interfaces.

When the firewall module comes online, the Network Management Processor (NMP) sends an SCP message that provides the secure VLANs that are defined for that particular firewall module.

If a VLAN is active and is displayed as a secure VLAN on one of the modules through the NMP CLIs, the information about the new active VLAN is sent to the Firewall Services Module.

The secure VLAN interface (SVI) is a Layer 3 secure VLAN interface between the module and the router on the supervisor engine, which allows them to communicate with each other.

One SVI is configured between each Firewall Services Module in the chassis and the supervisor engine module router. With software releases prior to Cisco IOS Release 12.2(14)SY and Catalyst operating system software version 7.6(1), only one SVI can exist between a given Firewall Services Module and the router on the supervisor engine.

Multiple VLAN interfaces are supported in Cisco IOS Release 12.2(14)SY with the **firewall multiple-vlan-interfaces** command and in the Catalyst operating system software version 7.6(1) with the **set firewall multiple-vlan-interfaces {enable|disable}** command.

**Note**

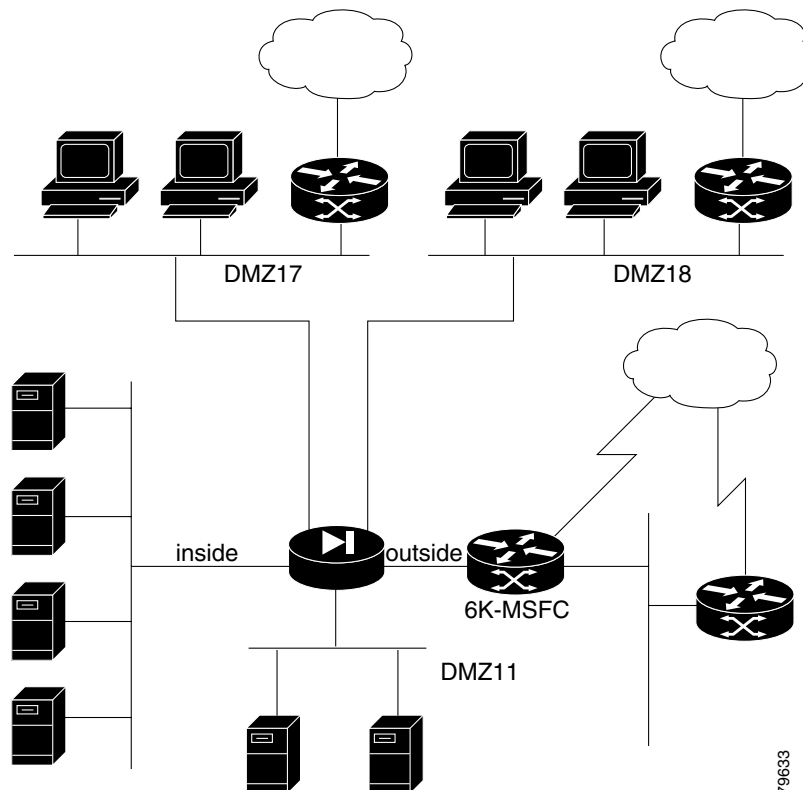
To prevent traffic from bypassing the firewall, policy-routing may be required when enabling support for multiple VLAN interfaces on the switch.

The Firewall Services Module configuration has the following characteristics:

- Each firewall interface is a Layer 3 interface.
- Each firewall interface has a fixed VLAN.
- The switch MSFC is used as a router connected to the module interfaces (SVI).
- The module views all networks (or subnetworks) beyond an interface as belonging to the same security level.
- Traffic from all of the non-firewall VLANs in the switch (those not recognized by the module) is routed through the MSFC without being stopped by the firewall.

You can configure the module in various situations by selecting the firewall features that meet the requirements of a particular network. [Figure 3-1](#) shows a typical firewall configuration.

**Figure 3-1 Firewall Configuration**



## Configuring the Switch Interface

This section describes the basic configuration steps performed on the switch and the Firewall Services Module.

### Cisco IOS Software

To set up the configuration on the switch using the Cisco IOS CLI, follow these general tasks:

	Command	Purpose
Step 1	Router# <b>configure terminal</b>	Enters VLAN configuration mode.
Step 2	Router(config)# <b>vlan</b> <i>vlan_number</i>	Creates VLANs.
Step 3	Router(config)# <b>interface vlan</b> <i>vlan_number</i>	Defines a controlled VLAN (SVI) on the MSFC (route processor).  <b>Note</b> You must configure a controlled VLAN (SVI) on the MSFC or you will be unable to configure VLANs on the module.
Step 4	Router(config)# <b>firewall multiple-vlan-interfaces</b>	Create multiple VLAN interfaces on the switch.
Step 5	Router(config)# <b>firewall vlan-group</b> <i>firewall_group</i> <i>vlan_range</i>	Creates a firewall group of controlled VLANs.
Step 6	Router(config) <b>firewall module</b> <i>module number</i> <b>vlan-group</b> <i>firewall_group</i>	Attaches the VLAN and firewall group to the slot where the module is located.
Step 7	Router(config)# <b>end</b> OR Router(vlan)# <b>exit</b>	Updates the VLAN database and returns to privileged EXEC mode.
Step 8	Router# <b>show firewall vlan-group</b>	Displays the firewall VLAN groups.
Step 9	Router# <b>show firewall module</b>	Displays the module configuration.
Step 10	Router# <b>show interface vlan</b> <i>vlan_number</i>	Displays the interface configuration.



#### Note

To prevent trunks from carrying firewall VLANs, enter this command:

```
switchport trunk allowed vlan {add | except | none | remove} vlan1, [, vlan [, vlan [,...]]]
```

This example shows how to configure the switch interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# vlan 55
Router(config-vlan)# vlan 56
Router(config-vlan)# vlan 57
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)# int vlan 55
Router(config-if)# ip address 55.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# end
Router# show firewall vlan-group
```

```

Group vlans
-----
    50 55-57
    51 70-85
Router# show firewall module
Module Vlan-groups
      8 50,51,
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
Router#

```

## Catalyst Operating System Software

To set up the configuration on the switch for the Firewall Services Module using the Catalyst operating system CLI, you must be in the proper VLAN Trunking Protocol (VTP) mode to create VLANs (server, transparent, or off modes all work) and then follow these general tasks:

:

	Command	Purpose
Step 1	Console> <b>enable</b>	Enters the switch configuration mode.
Step 2	Console>(enable) <b>set vlan</b> <i>vlan-number</i>	Create the VLAN.
Step 3	Console>(enable) <b>set vlan</b> <i>vlan_list</i> <b>firewall-vlan</b> <i>module</i>	Specifies firewall VLANs and maps them to the module.
Step 4	<b>set firewall multiple-vlan-interfaces</b> { <b>enable</b>   <b>disable</b> }	Create multiple VLAN interfaces on the switch.
Step 5	Console> <b>show vlan firewall-vlan</b> <i>module-number</i>	Displays the range of VLANs specified for the module.
Step 6	Console> <b>session 15</b>	(Optional) Accesses the MSFC (using the session 15 or session 16 command) enabling you to create the appropriate VLAN interfaces if desirable.

This example shows how to configure the switch interface:

```

Console>(enable) enable
Console>(enable) set vlan 7, 11-15, 19-20 firewall-vlan 8

```

```

Console> show vlan firewall-vlan 8
Console> show vlan fire 8
Secured vlans by firewall module 8:
7 11-15,19-20
Console>(enable) set vlan 8

```

## Sessioning into the Module

You can log into the module's maintenance partition or application partition.

### Sessioning into the Maintenance Partition

To log into the module's maintenance partition, perform these steps:

- Step 1** Telnet or log into the Catalyst 6500 series switch.
- Step 2** At the CLI prompt, session into the maintenance software by entering this command:

#### Cisco IOS:

```

Router# session slot number processor 1
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image

```



**Note** The processor should always be set at 1.

#### Catalyst Operating System:

```

Console> session module
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image

```

- Step 3** At the login prompt, enter **root**.
- Step 4** Enter the password for the account at the password prompt:

```
Password: cisco
```



**Note** If you have not changed the password from the factory-set default, a warning message is displayed. To change the password from the default, see the [“Changing and Recovering Passwords” section on page 5-11](#) for more information.

- Step 5** If the module does not boot into the maintenance partition, reset the module by entering the following command:

#### Cisco IOS:

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

#### Catalyst Operating System:

```

Console(enable)> reset module-number [boot device:partition]
Router# reboot

```

## Sessioning into the Application Partition

To log into the module's application partition, perform these steps:

**Step 1** Telnet or log into the Catalyst 6500 series switch.

**Step 2** At the CLI prompt, session into the application software by entering this command:

### Cisco IOS:

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x. You can also type 'exit'
at the remote
prompt to end the session Trying 127.0.0.81 ... Open

FWSM passwd:

Welcome to the FWSM firewall

Type help or '?' for a list of available commands.

FWSM>
```



**Note** The processor should always be set at 1.

### Catalyst Operating System:

```
Console (enable)# session module
```

**Step 3** If the module does not boot into the application partition, reset the module by entering the following command:

### Cisco IOS:

```
Router# hw-module module slot_number reset cf:4

Router# session slot module processor processor
```

### Catalyst Operating System:

```
Console (enable)# reset module cf:4
```

**Step 4** At the login prompt, enter your user name.

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

```
Password: password
```



**Note** If you have not changed the password from the factory-set default, a warning message is displayed. To change the password from the default, see the [“Changing and Recovering Passwords” section on page 5-11](#) for more information.

## Configuring the Module

To set up the configuration on the module, perform this task:

	Command	Purpose
Step 1	<code>FWSM(config)# hostname name</code>	Defines the host name in the command line prompt.
Step 2	<code>FWSM(config)# nameif vlan_number if_name security_level</code>	Specifies the interface name.
Step 3	<code>FWSM(config)# ip address if_name ip_address mask</code>	Defines a local address for each interface.
Step 4	<code>FWSM(config)# access-list acl_ID [deny   permit] protocol {source_addr   local_addr} {source_mask   local_mask} operator port {destination_addr   remote_addr} {destination_mask   remote_mask} operator port</code>	Defines an access list. Refer to <a href="#">Appendix B, “Command Reference”</a> and the “access-list” section on page B-2 and the “access-list (ospf)” section on page B-7.
Step 5	<code>FWSM(config)# access-group acl_ID in interface interface_name</code>	Defines access groups.
Step 6	<code>FWSM(config)# icmp permit any outside</code> <code>FWSM(config)# icmp permit any inside</code>	Allows connectivity testing between the switch and the FWSM.
Step 7	<code>FWSM(config)# show nameif</code>	Displays the configured interfaces.
Step 8	<code>FWSM(config)# show ip</code>	Displays the configured IP addresses.
Step 9	<code>FWSM(config)# show access-1</code>	Displays the configured access lists.



### Note

To allow traffic to flow from one interface to another, you must explicitly define an access list and map that access list to the appropriate interface. Unlike the PIX firewall, traffic from high-security level interfaces is not allowed to flow freely to an interface with a lower security level. By default, access lists are defined as **deny any any**.

This example shows how to configure the module:

```
FWSM(config)# hostname FWSM
FWSM(config)# nameif 55 outside 0
FWSM(config)# nameif 56 inside 100
FWSM(config)# ip address inside 10.1.1.1 255.255.255.0
FWSM(config)# ip address outside 55.1.1.2 255.255.255.0
FWSM(config)# access-list 1 permit ip any any
FWSM(config)# access-group 1 in interface inside
FWSM(config)# show nameif
nameif vlan55 inside security100
nameif vlan56 outside security0
FWSM(config)# show ip
System IP Addresses:
  ip address inside 10.1.1.1 255.255.255.0
  ip address outside 55.1.1.2 255.255.255.0
  ip address eobc 127.0.0.61 255.255.255.0
Current IP Addresses:
  ip address inside 10.1.1.1 255.255.255.0
  ip address outside 55.1.1.2 255.255.255.0
  ip address eobc 127.0.0.61 255.255.255.0
FWSM(config)# show access-list
access-list 1; 1 elements
access-list 1 permit ip any any (hitcnt=0)
```

```
FWSM(config)# show access-group
access-group 1 in interface inside
FWSM(config)#
```

## Saving the Configuration

To save your configuration, use one of the following methods:

- Store the configuration in Flash memory using the **write memory** command. You also can restore a configuration from Flash memory using the **configure memory** command.
- Store the configuration on a TFTP server using the **tftp-server** command to initially specify a host and the **write net** command to store the configuration.

To display your configuration, use one of the following methods:

- To list the stored configuration, use the **show configuration** command.
- To list the running configuration, use the **write terminal** command or **show running** command.

## Using PDM

Cisco PIX Device Manager (PDM) is a single-device graphical user interface (GUI) application that you can use to manage your Firewall Services Module. For detailed information about PDM, refer to the *Cisco PIX Device Manager Installation Guide, Version 2.1*.



### Note

PDM must be downloaded and installed for the Firewall Services Module release 1.1. You can download the image from CCO to upgrade PDM. Refer to [“Upgrading the PDM” section on page 3-10](#) for download and installation information.



### Note

The Firewall Services Module 1.1(2) software release is shipped with a preinstalled PDM 2.1 image. You can download the image from CCO to upgrade PDM if necessary. Refer to [“Upgrading the PDM” section on page 3-10](#) for download and installation information.



### Note

Be sure that you have configured the firewall VLAN (SVI) on the MSFC and that the module is recognized by the switch. Refer to [“Configuring the Switch Interface” section on page 3-3](#) for more information.

These sections describe the PDM and how to use it with your Firewall Services Module:

- [PDM Overview, page 3-9](#)
- [PDM Restrictions, page 3-9](#)
- [Platform and Browser Requirements, page 3-9](#)
- [Setting Up the Module for PDM, page 3-9](#)
- [Upgrading the PDM, page 3-10](#)
- [Starting PDM, page 3-11](#)

## PDM Overview

PDM is a signed Java applet that uses certificates and HTTP over SSL (HTTPS) to securely transmit all information between PDM and the Firewall Services Module. PDM performs the following functions:

- Configures your module without using the module CLI. You do not need to know the CLI commands to use PDM.
- Monitors the module with real-time graphs and data, including connection and throughput information. (You can also view up to five days of historical data.)
- Monitors and configures modules individually. You can point your browser to different modules and administer them from a single workstation.

## PDM Restrictions

These commands specific to the module are not supported by PDM 2.1:

- Any OSPF configuration commands; they are ignored but not changed by PDM.
- Any VPN configuration commands; they are ignored but not changed by PDM.

Refer to the PDM 2.1 release notes for the complete list of unsupported commands. The release notes are located at the following URL:

[http://cio.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v\\_21/pdmrn21/pdmrn21.htm](http://cio.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_21/pdmrn21/pdmrn21.htm)



**Note**

---

When running PDM 2.1 on the module, the Startup Wizard and VPN Wizard are not available.

---

## Platform and Browser Requirements

PDM is supported on the following platforms and browsers:

- Windows 2000, Windows NT 4.0, Windows 98, Windows ME, Windows XP Internet Explorer 5.0 or higher, or Netscape Navigator 4.51 or 4.7x, and at least 128 MB RAM
- Sun workstation with Solaris 2.6 or higher with Netscape Navigator 4.51 or 4.7x
- Red Hat Linux 7.0 or higher with Netscape Navigator 4.7x and at least 64 MB RAM

For details about PDM and its operation, refer to the *Cisco PIX Device Manager Installation Guide, Version 2.1*.

The installation guide is located at the following URL:

[http://cio.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v\\_21/pdmig/index.htm](http://cio.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_21/pdmig/index.htm)

## Setting Up the Module for PDM

Before you do this procedure, make sure you have installed the Firewall Services Module into the switch and you have completed the basic configuration described earlier in this chapter. Refer to the [“Configuration Overview” section on page 3-1](#).

To set up the module to use the PDM application, follow these steps:

- Step 1** Log into the Catalyst 6500 series switch where the Firewall Services Module is installed.
- Step 2** Enter the enable mode, and then enter the configuration mode.
- Step 3** Create a secure VLAN group by entering:

**Cisco IOS:**

```
Router# firewall vlan-group VLAN-group vlan-interfaces
```

**Catalyst Operating System**

```
Console>(enable) set vlan vlan-range firewall-vlan module-number
```

- Step 4** Map the secure VLAN group to the module by entering:

**Cisco IOS only:**

```
Router# firewall module module-number vlan-group VLAN-group
```

- Step 5** Telnet to the module and enter the enable mode, and then enter the configuration mode.
- Step 6** Run the setup CLI and follow the instructions as follows:

```
Router># enable
Password:
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# firewall vlan-group 5 10,20,50-51
Router(config)# firewall module 3 vlan-group 5
Router(config)# exit
Router# telnet 192.168.1.1
Trying 192.168.1.1 ... Open

FWSM passwd:
Welcome to the FWSM firewall

Type help or '?' for a list of available commands.
FWSM# enable
Password:
FWSM# configure terminal
FWSM(config)# setup
Pre-configure FWSM Firewall now through interactive prompts [yes]?
```

To complete this setup, follow the instructions that appear on the terminal.

## Upgrading the PDM

To install or upgrade PDM on the module, enter this command:

```
copy tftp://location/pathname flash:pdm
```

This example shows how to install or upgrade PDM on the module:

```
FWSM# copy tftp://10.1.1.1/pdm-211.bin flash:pdm
```

10.1.1.1 is the location of the TFTP server and the PDM image.

Verify that PDM was downloaded to the module.

## Starting PDM

To start PDM use the HTTP secure (**https**) command and enter the following address:

`https://IP address of FWSM`

This example shows how to start PDM:

**`https://192.168.1.1`**

192.168.1.1 is the IP address of one of the VLAN interfaces on the module.

You can now use the PDM 2.1 application to configure your Firewall Services Module. Access the PDM online help to use the application.

