Connecting to the Firewall Services Module and Managing the Configuration

This chapter tells how to access the Firewall Services Module (FWSM) command-line interface (CLI) and manage the configuration, and contains the following sections:

- Sessioning and Logging into the Firewall Services Module, page 3-1
- Managing the Configuration at the CLI, page 3-3

Sessioning and Logging into the Firewall Services Module

This section describes how to connect or "session," to the FWSM from the switch command line, log in, access privileged mode, and then configuration mode so you can configure the FWSM. The FWSM does not have an external console port, you must session into the FWSM for initial configuration. Later, when you configure interfaces and IP addresses on the FWSM itself, you can access the FWSM CLI remotely through an FWSM interface. See Chapter 11, "Allowing Remote Management," for more information.

Without any additional configuration for user authentication, the login method consists of logging in as the default user:

1. The login password lets you access unprivileged mode.
2. To access configuration commands, you must enter privileged mode, which requires a second password (privileged mode is also known as enable mode).
3. From privileged mode, you can access configuration mode, which does not require a password.

Caution Management access to the FWSM causes a degradation in performance. We recommend that you avoid accessing the FWSM when high network performance is critical.

Note For multiple context mode, see the "Logging into the FWSM in Multiple Context Mode" section on page 5-9 for more information about logging into security contexts.

This section describes how to log in as the default user. For information about advanced configuration options for login access, see the sections for the following features:

- User authentication for CLI access—See the "Configuring Authentication for CLI Access" section on page 12-8. You can configure user authentication for accessing the CLI from Telnet, SSH, and HTTP (for the PDM for FWSM). You can also require authentication for the **enable** command.
- Command authorization—See the "Configuring Command Authorization" section on page 12-10 or "Configuring TACACS+ Command Authorization" section on page 12-13. Use command authorization (the authority to enter commands) in conjunction with CLI or enable authentication.

To session into the FWSM, log in, access privileged mode, and then configuration mode, follow these steps:

Step 1 Session into the FWSM using the command appropriate for your switch operating system:

- Cisco IOS Software

```
Router# session slot number processor 1
```

- Catalyst OS

```
Console> (enable) session module_number
```

For multiple context mode, when you session into the FWSM, you access the system configuration. See Chapter 5, "Managing Security Contexts," for more information.

Step 2 Log into the FWSM by entering the login password at the following prompt:

```
FWSM passwd:
```

By default, the password is **cisco**.

To change the password, see the "Changing the Passwords" section on page 6-1.

Step 3 To access privileged mode, enter the following command:

```
FWSM> enable
```

This command accesses the highest privilege level.

The following prompt appears:

```
Password:
```

Step 4 Enter the enable password at the prompt.

By default, the password is blank, and you can press the **Enter** key to continue. See the "Changing the Passwords" section on page 6-1 to change the enable password.

The prompt changes to:

```
FWSM#
```

To exit privileged mode, enter **disable**. You can also enter **exit** or **quit** to exit the current access mode (privileged mode, configuration mode, etc.).

Step 5 To access configuration mode, enter the following command:

```
FWSM# configure terminal
```

The prompt changes to the following:

```
FWSM(config)#
```

Managing the Configuration at the CLI

The FWSM loads the configuration from a text file, called the startup configuration. This file resides in the **flash** partition. When you enter a command, the change is made only to the running configuration in memory. You must manually save the running configuration to the startup configuration for your changes to remain after a reboot.

The information in this section applies to both single and multiple security contexts, except where noted. Additional information about contexts is in Chapter 5, "Managing Security Contexts."

See the "Backing Up the Configuration" section on page 16-7 for more information about managing configuration files.

This section includes the following topics:

Saving Configuration Changes

To save your running configuration to the startup configuration, enter the following command:

```
FWSM# copy running-config startup-config
```

For multiple context mode, context startup configurations can reside on external servers. In this case, the FWSM saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not allow you to save the configuration to the server.

Note The **copy running-config startup-config** command is equivalent to the **write memory** command.

Viewing the Configuration

The following commands allow you to view the running and startup configurations.

- To view the running configuration, enter the following command:

```
FWSM# show running-config
```

- To view the startup configuration, enter the following command:

```
FWSM# show startup-config
```

Clearing and Removing Configuration Settings

To erase settings, enter one of the following commands.

- To clear all the configuration for a specified command and all its subcommands, enter the following command:

  ```
  FWSM# clear configurationcommand [subconfigurationcommand]
  ```

  This command clears all the current configuration for the specified configuration command. If you only want to clear the configuration for a specific subcommand, you can enter a value for *subconfigurationcommand*.

  For example, to clear the configuration for all **aaa** commands, enter the following command:

  ```
  FWSM# clear aaa
  ```

  To clear the configuration for only **aaa authentication** commands, enter the following command:

  ```
  FWSM# clear aaa authentication
  ```

- To disable the specific parameters or options of a command or subcommand, enter the following command:

  ```
  FWSM# no configurationcommand [subconfigurationcommand] qualifier
  ```

  In this case, you use the **no** command to remove the specific configuration identified by *qualifier*.

  For example, to remove a specific **nat** command, enter enough of the command to identify it uniquely as follows:

  ```
  FWSM# no nat (inside) 1
  ```

- To erase the startup configuration, enter the following command:

  ```
  FWSM# write erase
  ```

- To erase the running configuration, enter the following command:

  ```
  FWSM# clear configure all
  ```

Note In multiple context mode, if you enter **clear configure all** from the system configuration, you also remove all contexts and stop them from running.

Creating Text Configuration Files Offline

This guide describes how to use the CLI to configure the FWSM; when you save commands, the changes are written to a text file. Instead of using the CLI, however, you can edit a text file directly and paste a configuration at the configuration mode command-line prompt in its entirety, or line by line. Alternatively, you can download a text file to the FWSM Flash memory. See the "Downloading a Text Configuration" section on page 16-6 for information on downloading the configuration file to the FWSM.

In most cases, commands described in this guide are preceded by a CLI prompt. The prompt in the following example is "FWSM(config)#":

```
FWSM(config)# class gold
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted as follows:

```
class gold
```

See the "Text Configuration Files" section on page C-4 for more information about formatting the file.