CHAPTER 6

Configuring Basic Settings

This chapter tells how to configure basic settings on your Firewall Services Module (FWSM). This chapter includes the following sections:

Changing the Passwords

This section tells how to change the login password and enable password from their default settings, as well as how to change the maintenance partition passwords. The maintenance partition is used for troubleshooting, recovering from a corrupted image, or recovering lost passwords. See the following topics:

Note In multiple context mode, every context and the system execution space has its own login policies and passwords.

Changing the Login Password

By default, the login password is "cisco."

To change the password, enter the following command in privileged mode:

```
FWSM/contexta(config)# {passwd | password} password
```

You can enter **passwd** or **password**. The *password* is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Use the **clear password** command to restore the password to the default setting.

Changing the Enable Password

By default, the enable password is blank.

To change enable the password, enter the following command in privileged mode:

```
FWSM/contexta(config)# enable password password
```

The *password* is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

This command changes the password for the highest privilege level. If you configure local command authorization, you can set enable passwords for each privilege level from 0 to 15. See the "Configuring Command Authorization" section on page 12-10 for more information.

The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Enter the **enable password** command without a password to set the password to the default, which is blank.

Changing the Maintenance Partition Passwords

The maintenance partition is valuable for troubleshooting. For example, you can install new software to an application partition, reset passwords, or show crash dump information from the maintenance partition. You can only access the maintenance partition by sessioning into the FWSM (see the "Sessioning and Logging into the Firewall Services Module" section on page 3-1).

The maintenance partition has two user levels with different access privileges:

- root—Lets you configure the network partition parameters, upgrade the software images on the application partitions, change the guest account password, and enable or disable the guest account.

  The default password is "cisco."

- guest—Lets you configure the network partition parameters and show crash dump information.

  The default password is "cisco."

To change the maintenance partition passwords for both users, follow these steps:

Step 1 To reboot the FWSM into the maintenance partition, enter the command for your operating system:

- Cisco IOS software:

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

- Catalyst OS:

```
Console> (enable) reset mod_num boot cf:1
```

Step 2 To session into the FWSM, enter the command for your operating system:

- Cisco IOS software:

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

- Catalyst OS:

```
Console> (enable) session mod_num
```

Step 3 Log in as root by entering the following command:

```
Login: root
```

Step 4 Enter the password at the prompt:

```
Password:
```

The default password is “cisco”.

Step 5 Change the root password by entering the following command:

```
root@localhost# passwd
```

Step 6 Enter the new password at the prompt:

```
Changing password for user root
New password:
```

Step 7 Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

Step 8 Change the guest password by entering the following command:

```
root@localhost# passwd-guest
```

Step 9 Enter the new password at the prompt:

```
Changing password for user guest
New password:
```

Step 10 Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

This example shows how to set the password for the root account:

```
root@localhost# passwd
Changing password for user root
New password: *sh1p
Retype new password: *sh1p
passwd: all authentication tokens updated successfully
```

This example shows how to set the password for the guest account:

```
root@localhost# passwd-guest
Changing password for user guest
New password: f1rc8t
Retype new password: f1rc8t
passwd: all authentication tokens updated successfully
```

Setting the Host Name

When you set a host name for the FWSM, that name appears in the command line prompt. If you establish sessions to multiple devices, the host name helps you keep track of where you enter commands. By default, the host name is "FWSM".

For multiple context mode, the host name that you set in the system execution space appears in the command line prompt for all contexts.

The host name that you optionally set within a context does not appear in the command line, but is used for RSA key generation. If you do not set a host name within a context, the context name is used as the host name in the certificate. RSA keys are required for SSH, the HTTPS server, and can be used for VPN. You should also set the domain name for RSA key generation (see "Setting the Domain Name"). If you change the host name after you generate keys, you need to regenerate the keys using the **ca generate rsa key** command.

To specify the host name for the FWSM or for a context, enter the following command:

```
FWSM(config)# hostname name
```

This name can be up to 63 characters, including alphanumeric characters, spaces or any of the following special characters: ` ( ) + - , . / : = ?.

In single mode and in the system execution space in multiple mode, this name appears in the command line prompt. For example:

```
FWSM(config)# hostname farscape
farscape(config)#
```

For a context, this name is used for RSA key generation. If you do not set a host name within a context, the context name is used for the host name in the key. You can view a context host name using the **show hostname** command.

Setting the Domain Name

The domain name is used for RSA key generation. RSA keys are required for SSH, the HTTPS server, and can be used for VPN. You should also set the host name for key generation (see "Setting the Host Name"). If you change the domain name after generating keys, you need to regenerate the keys using the **ca generate rsa key** command.

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

To specify the domain name for the FWSM, enter the following command:

```
FWSM/contexta(config)# domain-name name
```

For example, to set the domain as cisco.com, enter the following command:

```
FWSM(config)# domain-name cisco.com
```

Adding a Login Banner

You can configure a message to display when a user connects to the FWSM, before a user logs in, or before a user enters privileged mode.

To configure a login banner, enter the following command in the system execution space or within a context:

```
FWSM/contexta(config)# banner {exec | login | motd} text
```

Adds a banner to display at one of three times: when a user first connects (message-of-the-day (**motd**)), when a user logs in (**login**), and when a user accesses privileged mode (**exec**). When a user connects to the FWSM, the message-of-the-day banner appears first, followed by the login banner and prompts. After the user successfully logs in to the FWSM, the exec banner displays.

For the banner text, spaces are allowed but tabs cannot be entered using the CLI. You can dynamically add the host name or domain name of the FWSM by including the strings **$(hostname)** and **$(domain)**. If you configure a banner in the system configuration, you can use that banner text within a context by using the **$(system)** string in the context configuration.

To add more than one line, precede each line by the **banner** command.

For example, to add a message-of-the-day banner, enter:

```
FWSM/contexta(config)# banner motd Welcome to the $(hostname) firewall.
FWSM/contexta(config)# banner motd Contact me at admin@admin.com for any
FWSM/contexta(config)# banner motd issues.
```

Configuring Interfaces

By default, all interfaces are enabled. For each interface, you must provide a name and a security level.

Note If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and stateful failover communications. See Chapter 15, "Using Failover," to configure the failover and state links.

This section includes the following topics:

Security Level Overview

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between Interfaces on the Same Security Level" section on page 6-8 for more information.

For interfaces that are on different security levels, the level controls the following behavior:

- NAT—When hosts on a higher security interface (inside) access hosts on a lower security interface (outside), you must configure Network Address Translation (NAT) for the inside hosts *or* specifically configure the inside hosts to bypass NAT.

  An inside host can communicate with the untranslated local address of the outside host without any special configuration on the outside interface. However, you can also optionally perform NAT on the outside network.

- Inspection engines—Some inspection engines are dependent on the security level:
  - SMTP inspection engine—Applied only for inbound connections (from lower level to higher level), which protects the SMTP servers on the higher security interface.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - XDMCP inspection engine—The XDMCP server can be configured only on the outside interface.
  - OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the FWSM.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).
- TCP intercept—The TCP intercept feature only applies to hosts or servers on a higher security level. See the "Other Protection Features" section on page 1-6 for more information about TCP intercept. This feature is configured using the *emb_limit* option in the **nat** and **static** commands.

- TCP sequence randomization—Each TCP connection has two Initial Sequence Numbers (ISNs): one generated by the client and one generated by the server. The FWSM randomizes the ISN that is generated by the host/server on the higher security interface. At least one of the ISNs must be randomly generated so that attackers cannot predict the next ISN and potentially hijack the session.
- Maximum connections limit—You can set a limit on the number of TCP and UDP connections allowed through the FWSM, but only connections from a higher security interface to a lower security interface are tracked. This limit is set using the *max_conns* option in the **nat** and **static** commands.
- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

These behaviors do not affect interfaces that are on the same security level. For example, you do not have to perform NAT, nor do you have to configure the interfaces to bypass NAT. You can, however, optionally configure NAT for these interfaces. Similarly, inspection engines are applied to both interfaces, as is filtering.

Note By default, the Cisco PIX firewall allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). However, the FWSM does not allow any traffic to pass between interfaces unless you explicitly permit it with an access control list (ACL). While you still have to specify the security level for an interface on the FWSM, the security level does not provide an explicit permission for traffic to travel from a high security interface to a low security interface.

Setting the Name and Security Level

By default, all interfaces are enabled. However, you must assign a name and security level to each interface before you can fully configure the FWSM. Many commands use the interface name instead of the interface (VLAN) ID.

You can assign a name to a VLAN that has not yet been assigned to the FWSM (see the "Assigning VLANs to the Firewall Services Module" section on page 2-2), but you see a warning message.

Note If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and stateful failover communications. See Chapter 15, "Using Failover," to configure the failover and state links.

For multiple context mode, follow these guidelines:

- Configure the context interfaces from within each context.
- You can only configure context interfaces that you already assigned to the context in the system configuration.
- The system configuration does not include configurable interfaces, except for failover interfaces. Do not configure failover interfaces with this procedure. See Chapter 15, "Using Failover," for more information.

In transparent firewall mode, you can use only two interfaces, one inside and one outside.

Note If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

To name an interface, enter the following command:

```
FWSM/contexta(config)# nameif {vlan n | context_map_name} name [security]n
```

For multiple context mode, if you gave the VLAN interface a mapped name for the context in the system configuration, then you must use the mapped name.

The *name* is a text string up to 48 characters, and is not case-sensitive.

The security level is an integer between 0 and 100. 0 is the least secure and 100 the most secure. You can optionally include the word **security** before the level number to make your configuration easier to read. To assign more than one interface to the same level, see the "Allowing Communication Between Interfaces on the Same Security Level" section on page 6-8 to enable this feature.

For example, enter the **show nameif** command to view the interface names:

```
FWSM# show nameif
nameif vlan100 outside security0
nameif vlan101 inside security100
nameif vlan102 dmz security50
```

Allowing Communication Between Interfaces on the Same Security Level

By default, interfaces on the same security level cannot communicate with each other, even if you configure NAT and ACLs.

Allowing communication between same security interfaces provides the following benefits:

- You do not need to configure NAT between same security interfaces.

  You can, however, configure NAT if desired. If you configure dynamic NAT for an interface, then to allow connections initiated from another interface, even if it is on the same security level, you need to configure static NAT.

  If you want to configure connection limits but do not want to configure NAT (where connection limits are set), you can configure identity NAT or NAT exemption. (See the "Configuring Connection Limits for Non-NAT Configurations" section on page 6-9 or the "Bypassing NAT" section on page 9-29.)

- You can configure more than 101 communicating interfaces.

  If you use different levels for each interface, you can configure only one interface per level (0 to 100).

- You want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

  For different security level interfaces, many protection features apply only in one direction, for example, inspection engines, TCP intercept, and connection limits.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

To enable interfaces on the same security level so that they can communicate with each other, enter the following command:

```
FWSM/contexta(config)# same-security-traffic permit inter-interface
```

To disable this setting, add **no** before the command.

Turning Off and Turning On Interfaces

All interfaces are enabled by default. If you disable or reenable the interface within a context, only that context interface is affected. But if you disable or reenable the interface in the system execution space, then you affect that VLAN interface for all contexts.

To disable an interface or reenable it, follow these steps:

Step 1 To enter the interface configuration mode, enter the following command:

```
FWSM/contexta(config)# interface interface_name
```

Step 2 To disable the interface, enter the following command:

```
FWSM/contexta(config-interface)# shutdown
```

Step 3 To reenable the interface, enter the following command:

```
FWSM/contexta(config-interface)# no shutdown
```

Configuring Connection Limits for Non-NAT Configurations

Transparent firewall mode

Same security level mode

The NAT configuration enables you to set connection limits for traffic. For transparent firewall mode or for same security interfaces on which you do not want to configure NAT (see the "Allowing Communication Between Interfaces on the Same Security Level" section on page 6-8), you can configure identity NAT to set these limits. Identity NAT lets you specify the addresses for which you want to set limits, but no translation is performed. (For same security interfaces, you can configure any method for bypassing NAT, including NAT exemption. See the "Bypassing NAT" section on page 9-29 for more information. For transparent mode, the FWSM supports only the following method.)

To set connection limits for the inside interface (transparent mode) or for any same security interface, enter the following command:

```
FWSM/contexta(config)# static (inside_interface,outside_interface) local_ip_address
local_ip_address netmask mask [norandomseq] [[tcp] tcp_max_conns [emb_limit]]
[udp udp_max_conns]
```

Enter the same IP address for both *local_ip_address* options.

Set one or more of the following options:

- **norandomseq—**No TCP Initial Sequence Number (ISN) randomization. Only use this option if another in-line firewall is also randomizing sequence numbers and the result is scrambling the data. See the "Security Level Overview" section on page 6-6 for information about TCP sequence numbers.
- **tcp** *tcp_max_conns,* **udp** *udp_max_conns*—The maximum number of simultaneous TCP and/or UDP connections for the entire subnet up to 65,536. The default is 0 for both protocols, which means the maximum connections.
- *emb_limit*—The maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. (See the "Other Protection Features" section on page 1-6 for more information.) The default is **0**, which means the maximum embryonic connections. You must enter the **tcp** *tcp_max_conns* before you enter the *emb_limit*. If you want to use the default value for *tcp_max_conns*, but change the *emb_limit*, then enter **0** for *tcp_max_conns*.

For example, to set options for the host 10.1.1.1, enter the following command:

```
FWSM/contexta(config)# static (inside,outside) 10.1.1.1 10.1.1.1 netmask 255.255.255.255
norandomseq tcp 1000 200 udp 1000
```