CHAPTER 11

Allowing Remote Management

This chapter describes how to allow remote access to the Firewall Services Module (FWSM) CLI and how to allow ICMP to and from the FWSM.

Caution Management access to the FWSM using Telnet, SSH, or HTTPS might cause a degradation in performance depending on the commands that you execute during the session. For example, if there are 50,000 current connections and you enter the **show conn** command, the CPU utilization is higher than if you do not enter the command. We recommend that you avoid executing commands on the FWSM when high network performance is critical.

This chapter includes the following sections:

Note To "session" into the FWSM from the switch, see the "Sessioning and Logging into the Firewall Services Module" section on page 3-1.

Allowing Telnet

The FWSM allows Telnet connections to the FWSM for management purposes. You cannot use Telnet to the lowest security interface unless you use Telnet inside an IPSec tunnel (See the "Allowing a VPN Management Connection" section on page 11-5).

You can control the number of Telnet sessions allowed per context using resource classes (see the "Configuring a Class" section on page 5-14). The FWSM allows a maximum of 5 concurrent Telnet connections per context, if available, with a maximum of 100 connections divided between all contexts. See the "Rule Limits" section on page A-5 for information about the maximum number of Telnet rules allowed for the entire system.

To configure Telnet access to the FWSM, follow these steps:

Step 1 To identify the IP addresses from which the FWSM accepts connections, enter the following command for each address or subnet:

```
FWSM/contexta(config)# telnet source_IP_address mask source_interface
```

The *source_interface* cannot be the lowest security interface unless you use Telnet inside an IPSec tunnel (See the "Allowing a VPN Management Connection" section on page 11-5).

For example, you must configure at least two interfaces so the FWSM can determine the lowest security interface. If you configure a single interface (for the admin context, for example), then that interface is both the highest and the lowest security interface and cannot be used. Similarly, if all interfaces are on the same security level, you cannot use Telnet.

Step 2 (Optional) To set the duration for how long a Telnet session can be idle before the FWSM disconnects the session, enter the following command:

```
FWSM/contexta(config)# telnet timeout minutes
```

Set the timeout from 1 to 1440 minutes. The default is 5 minutes. The default duration is too short in most cases and should be increased until all pre-production testing and troubleshooting has been completed.

For example, to let a host on the inside interface with an address of 192.168.1.2 access the FWSM, enter the following command:

```
FWSM/contexta(config)# telnet 192.168.1.2 255.255.255.255 inside
FWSM/contexta(config)# telnet timeout 30
```

To allow all users on the 192.168.3.0 network to access the FWSM on the inside interface, enter the following command:

```
FWSM/contexta(config)# telnet 192.168.3.0 255.255.255.0 inside
```

Allowing SSH

The FWSM allows SSH connections to the FWSM for management purposes. You can control the number of SSH sessions allowed per context using resource classes (see the "Configuring a Class" section on page 5-14). The FWSM allows a maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided between all contexts. See the "Rule Limits" section on page A-5 for information about the maximum number of SSH rules allowed for the entire system.

SSH is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. FWSM supports the SSH remote shell functionality provided in SSH Version 1 and supports DES and 3DES ciphers.

Note SSH v1.*x* and v2 are entirely different protocols and are not compatible. Make sure that you download a client that supports SSH v1.*x*.

This section includes the following topics:

Configuring SSH Access

To configure SSH access to the FWSM, follow these steps:

Step 1 To generate an RSA key pair, which is required for SSH, enter the following command:

```
FWSM/contexta(config)# ca generate rsa key modulus
```

The modulus (in bits) is 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. We recommend a value of 768.

Before you generate the key, you should set the host name and the domain name according to the "Setting the Host Name" section on page 6-4 and the "Setting the Domain Name" section on page 6-5. These settings are used in the key.

Step 2 To save the RSA keys to persistent Flash memory, enter the following command:

```
FWSM/contexta(config)# ca save all
```

Step 3 To identify the IP addresses from which the FWSM accepts connections, enter the following command for each address or subnet:

```
FWSM/contexta(config)# ssh source_IP_address mask source_interface
```

The FWSM accepts SSH connections from all interfaces, including the lowest security one.

Step 4 (Optional) To set the duration for how long an SSH session can be idle before the FWSM disconnects the session, enter the following command:

```
FWSM/contexta(config)# ssh timeout minutes
```

Set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases and should be increased until all pre-production testing and troubleshooting has been completed.

For example, to generate RSA keys and let a host on the inside interface with an address of 192.168.1.2 access the FWSM, enter the following command:

```
FWSM/contexta(config)# ca generate rsa key 1024
FWSM/contexta(config)# ca save all
FWSM/contexta(config)# ssh 192.168.1.2 255.255.255.255 inside
FWSM/contexta(config)# ssh 192.168.1.2 255.255.255.255 inside
FWSM/contexta(config)# ssh timeout 30
```

To allow all users on the 192.168.3.0 network to access the FWSM on the inside interface, the following command:

```
FWSM/contexta(config)# ssh 192.168.3.0 255.255.255.0 inside
```

Using an SSH Client

To gain access to the FWSM console using SSH, at the SSH client enter the username **pix** and enter the login password set by the **password** command (see the "Changing the Login Password" section on page 6-2). For individual logins, see the "Configuring Authentication for CLI Access" section on page 12-8.

When starting an SSH session, a dot (.) displays on the FWSM console before the SSH user authentication prompt appears, as follows:

```
FWSM/contexta(config)# .
```

The display of the dot does not affect the functionality of SSH. The dot appears at the console when generating a server key or decrypting a message using private keys during SSH key exchange before user authentication occurs. These tasks can take up to two minutes or longer. The dot is a progress indicator that verifies that the FWSM is busy and has not hung.

Allowing HTTPS for PDM

To use PDM, you need to enable the HTTPS server, allow HTTPS connections to the FWSM, and enable the PDM metrics history. All of these tasks are completed if you use the **setup** command. This section describes how to manually configure PDM access.

The FWSM allows a maximum of 5 concurrent HTTPS connections per context, if available, with a maximum of 16 connections divided between all contexts. See the "Rule Limits" section on page A-5 for information about the maximum number of HTTPS rules allowed for the entire system.

To configure PDM access, follow these steps:

Step 1 To generate an RSA key pair, which is required for HTTPS, enter the following command:

```
FWSM/contexta(config)# ca generate rsa key modulus
```

The modulus (in bits) is 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. We recommend a value of 768.

Before you generate the key, you should set the host name and the domain name according to the "Setting the Host Name" section on page 6-4 and the "Setting the Domain Name" section on page 6-5. These settings are used in the key.

Step 2 To save the RSA keys to persistent Flash memory, enter the following command:

```
FWSM/contexta(config)# ca save all
```

Step 3 To identify the IP addresses from which the FWSM accepts HTTPS connections, enter the following command for each address or subnet:

```
FWSM/contexta(config)# http source_IP_address mask source_interface
```

Step 4 To enable the HTTPS server, enter the following command:

```
FWSM/contexta(config)# http server enable
```

Step 5 To enable PDM metrics history, enter the following command:

```
FWSM/contexta(config)# pdm history enable
```

For example, to enable the HTTPS server and let a host on the inside interface with an address of 192.168.1.2 access PDM, enter the following commands:

```
FWSM/contexta(config)# ca generate rsa key 1024
FWSM/contexta(config)# ca save all
FWSM/contexta(config)# http server enable
FWSM/contexta(config)# pdm history enable
FWSM/contexta(config)# http 192.168.1.2 255.255.255.255 inside
```

To allow all users on the 192.168.3.0 network to access PDM on the inside interface, enter the following command:

```
FWSM/contexta(config)# http 192.168.3.0 255.255.255.0 inside
```

Allowing a VPN Management Connection

The FWSM supports IPSec for management access. An IPSec virtual private network (VPN) ensures that IP packets can safely travel over insecure networks such as the Internet. All communication between two VPN peers occurs over a secure tunnel, which means the packets are encrypted and authenticated by the peers.

The FWSM can connect to another VPN concentrator, such as a Cisco PIX firewall or a Cisco IOS router, using a site-to-site tunnel. You specify the peer networks that can communicate over the tunnel. In the case of the FWSM, the only address available on the FWSM end of the tunnel is the interface itself.

The FWSM can also accept connections from VPN clients, either hosts running the Cisco VPN client, or VPN concentrators such as the Cisco PIX firewall or Cisco IOS router running the Easy VPN client. Unlike a site-to-site tunnel, you do not know in advance the IP address of the client. Instead, you rely on client authentication.

The FWSM can support 5 concurrent IPSec connections, with a maximum of 10 concurrent connections divided between all contexts. You can control the number of IPSec sessions allowed per context using resource classes (see the "Configuring a Class" section on page 5-14).

This section describes the following topics:

Configuring Basic Settings for All Tunnels

The following steps are required for both VPN client access and for site-to-site tunnels, and include setting the Internet Key Exchange (IKE) policy (IKE is part of the Internet Security Association and Key Management Protocol (ISAKMP)) and the IPSec transforms:

Step 1 To set the IKE encryption algorithm, enter the following command:

```
FWSM/contexta(config)# isakmp policy priority encryption {des | 3des}
```

The **3des** keyword is more secure than **des**.

You can have multiple IKE policies. The FWSM tries each policy in order of the *priority* until the policy matches the peer policy. The *priority* can be an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest. Use this same priority number for the following **isakmp** commands.

Step 2 To set the Diffie-Hellman group used for key exchange, enter the following command:

```
FWSM/contexta(config)# isakmp policy priority group {1 | 2}
```

Group 1 is 768 bits, and Group 2 is 1024 bits (and therefore more secure).

Step 3 To set the authentication algorithm, enter the following command:

```
FWSM/contexta(config)# isakmp policy priority hash {md5 | sha}
```

The **sha** keyword is more secure than **md5**.

Step 4 To set the IKE authentication method as a shared key, enter the following command:

```
FWSM/contexta(config)# isakmp policy priority authentication pre-share
```

You can alternatively use certificates instead of a shared key by specifying the **rsa-sig** option. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information about this method.

Step 5 To enable IKE on the tunnel interface, enter the following command:

```
FWSM/contexta(config)# isakmp enable interface_name
```

Step 6 To set the authentication and encryption methods used for IPSec tunnels in a transform set, enter the following command:

```
FWSM/contexta(config)# crypto ipsec transform-set transform_name {[ah-md5-hmac |
ah-sha-hmac] | [esp-md5-hmac | esp-sha-hmac]} {esp-des | esp-3des}
```

You refer to this transform set when you configure the VPN client group or a site-to-site tunnel.

You can refer to up to 6 transform sets for the tunnel, and the sets are checked in order until the transforms match.

The authentication and encryption algorithms of this transform typically match the IKE policy (**isakmp policy** commands). For site-to-site tunnels, this transform must match the peer transform.

Typically, you need to specify one authentication option and one encryption option.

Authentication options include the following (from most secure to least secure):

- **ah-sha-hmac**
- **ah-md5-hmac**
- **esp-sha-hmac**
- **esp-md5-hmac**

Encryption options include the following (from most secure to least secure):

- **esp-3des**
- **esp-des**

Note **esp-null** (no encryption) is for testing purposes only.

Although you can specify authentication alone, or encryption alone, these methods are not secure. You can also specify two authentication options, but this method does not increase security and also slows down the FWSM because each packet is authenticated two times.

For example, to configure the IKE policy and the IPSec transform sets, enter the following commands:

```
FWSM/contexta(config)# isakmp policy 1 authentication pre-share
FWSM/contexta(config)# isakmp policy 1 encryption 3des
FWSM/contexta(config)# isakmp policy 1 group 2
FWSM/contexta(config)# isakmp policy 1 hash sha
FWSM/contexta(config)# isakmp enable outside
FWSM/contexta(config)# crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
FWSM/contexta(config)# crypto ipsec transform-set site_to_site esp-3des ah-sha-hmac
```

Configuring VPN Client Access

A host with an installed version of the Cisco VPN Client can connect to the FWSM for management purposes over a public network, such as the Internet.

To allow remote clients to connect to the FWSM for management access, first configure basic VPN settings (see "Configuring Basic Settings for All Tunnels"), and then follow these steps:

Step 1 To specify the transform sets (defined in the "Configuring Basic Settings for All Tunnels" section on page 11-5) allowed for client tunnels, enter the following command:

```
FWSM/contexta(config)# crypto dynamic-map dynamic_map_name priority set transform-set
transform_set1 [transform_set2] [...]
```

List multiple transform sets in order of priority (highest priority first).

This dynamic crypto map allows unknown IP addresses to connect to the FWSM.

The **dynamic-map** name is used in Step 2.

The *priority* specifies the order in which multiple commands are evaluated. If you have a command that specifies one set of transforms, and another that specifies others, then the priority number determines the command that is evaluated first.

Step 2 To assign the dynamic crypto map (from Step 1) to a static tunnel, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name priority ipsec-isakmp dynamic
dynamic_map_name
```

Step 3 To specify the interface at which you want the client tunnels to terminate, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name interface interface_name
```

You can apply only one **crypto map** name to an interface, so if you want to terminate both a site-to-site tunnel and VPN clients on the same interface, they need to share the same **crypto map** name.

Step 4 To specify the AAA server or the local user database that provides user authentication when a client connects to the FWSM, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name client authentication
{LOCAL | aaa_server_name [LOCAL]}
```

You must first configure the server name according to the "Identifying a AAA Server" section on page 12-6 or the local database according to the "Configuring the Local Database" section on page 12-6.

Step 5 To specify the range of addresses that VPN clients use on the FWSM enter the following command:

```
FWSM/contexta(config)# ip local pool pool_name ip_address[-ip_address]
```

All tunneled packets from the client use one of these addresses as the source address.

Step 6 To specify the traffic that is destined for the FWSM, so you can tunnel only that traffic according to the **vpngroup split-tunnel** command in Step 8, enter the following command:

```
FWSM/contexta(config)# access-list acl_name [extended] permit {protocol} host
fwsm_interface_address pool_addresses mask
```

This ACL identifies traffic from the local pool (see Step 5) destined for the FWSM interface. See the "Adding an Extended Access Control List" section on page 10-13 for more information about ACLs.

Step 7 To assign the VPN address pool to a VPN group, enter the following command:

```
FWSM/contexta(config)# vpngroup group_name address-pool pool_name
```

This group specifies VPN characteristics for connecting clients. When a client connects the FWSM, they need to enter the VPN group name as well as the VPN group password in Step 9.

Step 8 To specify that only traffic destined for the FWSM is tunneled, enter the following command:

```
FWSM/contexta(config)# vpngroup group_name split-tunnel acl_name
```

This command is required.

Step 9 To set the VPN group password, enter the following command:

```
FWSM/contexta(config)# vpngroup group_name password password
```

Step 10 To allow Telnet or SSH access, see the "Allowing Telnet" section on page 11-1 and the "Allowing SSH" section on page 11-2.

Specify the VPN pool addresses in the **telnet** and **ssh** commands.

For example, the following commands allow VPN clients to use Telnet on the outside interface (209.165.200.225). The user authentication is the local database, so users with the VPN group name and password, as well as the username "admin" and the password "passw0rd" can connect to the FWSM.

```
FWSM/contexta(config)# isakmp policy 1 authentication pre-share
FWSM/contexta(config)# isakmp policy 1 encryption 3des
FWSM/contexta(config)# isakmp policy 1 group 2
FWSM/contexta(config)# isakmp policy 1 hash sha
FWSM/contexta(config)# isakmp enable outside
FWSM/contexta(config)# username admin password passw0rd
FWSM/contexta(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
FWSM/contexta(config)# crypto dynamic-map vpn_client 1 set transform-set vpn
FWSM/contexta(config)# crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
FWSM/contexta(config)# crypto map telnet_tunnel interface outside
FWSM/contexta(config)# crypto map telnet_tunnel client authentication LOCAL
FWSM/contexta(config)# ip local pool client_pool 10.1.1.1-10.1.1.2
FWSM/contexta(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host
10.1.1.1
FWSM/contexta(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host
10.1.1.2
FWSM/contexta(config)# vpngroup admin address-pool client_pool
FWSM/contexta(config)# vpngroup admin split-tunnel VPN_SPLIT
FWSM/contexta(config)# vpngroup admin password $ecure23
FWSM/contexta(config)# telnet 10.1.1.1 255.255.255.255 outside
FWSM/contexta(config)# telnet 10.1.1.2 255.255.255.255 outside
FWSM/contexta(config)# telnet timeout 30
```

Configuring a Site-to-Site Tunnel

To configure a site-to-site tunnel, first configure basic VPN settings (see "Configuring Basic Settings for All Tunnels"), and then follow these steps:

Step 1 To set the shared key used by both peers, enter the following command:

```
FWSM/contexta(config)# isakmp key keystring address peer-address
```

Step 2 To identify the traffic allowed to go over the tunnel, enter the following command:

```
FWSM/contexta(config)# access-list acl_name [extended] {deny | permit} {protocol} host
fwsm_interface_address dest_address mask
```

For the destination address, specify the addresses that are allowed to access the FWSM.

See the "Adding an Extended Access Control List" section on page 10-13 for more information about ACLs.

Step 3 To create an IPSec tunnel, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name priority ipsec-isakmp
```

All tunnel attributes are identified by the same **crypto map** name.

The *priority* specifies the order in which multiple commands are evaluated. If you have a command for this **crypto map** name that specifies **ipsec-isakmp**, and another that specifies **ipsec-isakmp dynamic** (for VPN client connections), then the priority number determines the command that is evaluated first.

Step 4 To assign the ACL from Step 2 to this tunnel, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name priority match address acl_name
```

Step 5 To specify the remote peer on which this tunnel terminates, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name priority set peer ip_address
```

Step 6 To specify the transform sets for this tunnel (defined in the "Configuring Basic Settings for All Tunnels" section on page 11-5), enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name priority set transform-set
transform_set1 [transform_set2] [...]
```

List multiple transform sets in order of priority (highest priority first). You can specify up to six transform sets.

Step 7 To specify the interface at which you want this tunnel to terminate, enter the following command:

```
FWSM/contexta(config)# crypto map crypto_map_name interface interface_name
```

You can apply only one **crypto map** name to an interface, so if you want to terminate both a site-to-site tunnel and VPN clients on the same interface, they need to share the same **crypto map** name.

This command must be entered after all other **crypto map** commands. If you change any **crypto map** settings, remove this command with the **no** prefix, and reenter it.

Step 8 To allow Telnet or SSH access, see the "Allowing Telnet" section on page 11-1 and the "Allowing SSH" section on page 11-2.

For example, the following commands allow hosts connected to the peer router (209.165.202.129) to use Telnet on the outside interface (209.165.200.225).

```
FWSM/contexta(config)# isakmp policy 1 authentication pre-share
FWSM/contexta(config)# isakmp policy 1 encryption 3des
FWSM/contexta(config)# isakmp policy 1 group 2
FWSM/contexta(config)# isakmp policy 1 hash sha
FWSM/contexta(config)# isakmp enable outside
FWSM/contexta(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
FWSM/contexta(config)# isakmp key 7mfi02lirotn address 209.165.200.223
FWSM/contexta(config)# access-list TUNNEL extended permit ip host 209.165.200.225
209.165.201.0 255.255.255.224
FWSM/contexta(config)# crypto map telnet_tunnel 2 ipsec-isakmp
FWSM/contexta(config)# crypto map telnet_tunnel 1 match address TUNNEL
```

```
FWSM/contexta(config)# crypto map telnet_tunnel 1 set peer 209.165.202.129
FWSM/contexta(config)# crypto map telnet_tunnel 1 set transform-set vpn
FWSM/contexta(config)# crypto map telnet_tunnel interface outside
FWSM/contexta(config)# telnet 209.165.201.0 255.255.255.224 outside
FWSM/contexta(config)# telnet timeout 30
```

Allowing ICMP to and from the FWSM

By default, ICMP (including ping) is not allowed to an FWSM interface (or through the FWSM. To allow ICMP *through* the FWSM, see Chapter 10, "Controlling Network Access with Access Control Lists."). ICMP is an important tool for testing your network connectivity; however, it can also be used to attack the FWSM or your network. We recommend allowing ICMP during your initial testing, but then disallowing it during normal operation.

See the "Rule Limits" section on page A-5 for information about the maximum number of ICMP rules allowed for the entire system.

To permit or deny address(es) to reach an FWSM interface with ICMP (either from a host to the FWSM, or from the FWSM to a host, which requires the ICMP reply to be allowed back), enter the following command:

```
FWSM/contexta(config)# icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

If you do not specify an *icmp_type*, all types are identified. You can enter the number or the name. To control ping, specify **echo-reply** (**0**) (FWSM to host) or **echo** (**8**) (host to FWSM). See the "ICMP Types" section on page D-9 for a list of ICMP types.

Like ACLs, the FWSM matches a packet to each **icmp** statement in order. You should use specific statements first, and general statements later. There is an implicit deny at the end. For example, if you allow all addresses first, then deny a specific address after, then that address will be unintentionally allowed because it matched the first statement.

Note If you only want to allow the FWSM to ping a host (and thus allow the echo reply back to the interface), and not allow hosts to ping the FWSM, you can enable the ICMP inspection engine instead of entering the command above. See the "ICMP Inspection Engine" section on page 13-10.

For example, to allow all hosts except the one at 10.1.1.15 to use ICMP to the inside interface, enter the following commands:

```
FWSM/contexta(config)# icmp deny host 10.1.1.15 inside
FWSM/contexta(config)# icmp permit any inside
```

To allow the host at 10.1.1.15 to use only ping to the inside interface, enter the following commands:

```
FWSM/contexta(config)# icmp permit host 10.1.1.15 inside
```