



## CHAPTER 6

# Configuring Interface Parameters

---

This chapter describes how to configure each interface for a name, security level, and IP address. For transparent firewall, you also need to configure a bridge group for each interface pair.

This chapter includes the following sections:

- [Security Level Overview, page 6-1](#)
- [Configuring Interfaces for Routed Firewall Mode, page 6-2](#)
- [Configuring Interfaces for Transparent Firewall Mode, page 6-3](#)
- [Allowing Communication Between Interfaces on the Same Security Level, page 6-5](#)
- [Turning Off and Turning On Interfaces, page 6-6](#)

## 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 6-5 for more information.

The level controls the following behavior:

- Inspection engines—Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - 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. For same security interfaces, you can filter traffic in either direction.
- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **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.

For some security interfaces, you can configure **established** commands for both directions.

## Configuring Interfaces for Routed Firewall Mode

Before you can allow traffic through the FWSM, you need to configure an interface name and an IP address. You should also change the security level from the default, which is 0. If you name an interface “inside” and you do not set the security level explicitly, then the FWSM sets the security level to 100.



### 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 13, “Configuring 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 only lets you configure failover interfaces; do not configure failover interfaces with this procedure. See [Chapter 13, “Configuring Failover,”](#) for more information.
- 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 connections using the **clear local-host** command.

You can add any VLAN ID to the configuration, but only VLANs that are assigned to the FWSM by the switch can pass traffic. To view all VLANs assigned to the FWSM, use the **show vlan** command.

To configure an interface, perform the following steps:

**Step 1** To specify the interface you want to configure, enter the following command:

```
hostname(config)# interface {vlan number | mapped_name}
```

In multiple context mode, enter the mapped name if one was assigned using the **allocate-interface** command.

For example, enter the following command:

```
hostname(config)# interface vlan 101
```

**Step 2** To name the interface, enter the following command:

```
hostname(config-if)# nameif name
```

The *name* is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the **no** form, because that command causes all commands that refer to that name to be deleted.



### Note

After you set the name for an interface, the security-level is automatically changed to 0. However, if the name is “inside,” then the security level becomes 100.

**Step 3** To set the security level, enter the following command:

```
hostname(config-if)# security-level number
```

Where *number* is an integer between 0 (lowest) and 100 (highest).

**Step 4** To set the IP address, enter the following command:

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

The **standby** keyword and address is used for failover. See [Chapter 13, “Configuring Failover,”](#) for more information.



**Note** To set an IPv6 address, see the [“Configuring IPv6 on an Interface”](#) section on page 9-2.

The following example configures parameters for VLAN 101:

```
hostname(config)# interface vlan 101
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
```

The following example configures parameters in multiple context mode for the context configuration. The interface ID is a mapped name.

```
hostname/contextA(config)# interface int1
hostname/contextA(config-if)# nameif outside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

## Configuring Interfaces for Transparent Firewall Mode

Before you can allow traffic through the FWSM, you need to configure an interface name, security level, and bridge group association. Finally, assign a management IP address for each bridge group. This section includes the following topics:

- [Configuring Transparent Firewall Interface Parameters, page 6-3](#)
- [Assigning an IP Address to a Bridge Group, page 6-5](#)

## Configuring Transparent Firewall Interface Parameters

A transparent firewall connects the same network on its inside and outside interfaces. Each pair of interfaces belongs to a bridge group, to which you must assign a management IP address (see the [“Assigning an IP Address to a Bridge Group”](#) section on page 6-5). You can configure up to eight bridge groups of two interfaces each. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.



**Note** The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a system log server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

**Note**

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications.

For multiple context mode, follow these guidelines for configuring interfaces:

- You must 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 only lets you configure failover interfaces; do not configure failover interfaces with this procedure.
- 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 connections using the **clear local-host** command.

You can add any VLAN ID to the configuration, but only VLANs that are assigned to the FWSM by the switch can pass traffic. To view all VLANs assigned to the FWSM, use the **show vlan** command.

To assign an interface to a bridge group, set the name, and set the security level, perform the following steps:

**Step 1** To identify the interface, enter the following command:

```
hostname(config)# interface {vlan number | mapped_name}
```

In multiple context mode, enter the mapped name if one was assigned using the **allocate-interface** command.

**Step 2** To assign it to a bridge group, enter the following command:

```
hostname(config-if)# bridge-group number
```

Where *number* is an integer between 1 and 100. You can only assign two interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.

**Step 3** To name the interface, enter the following command:

```
hostname(config-if)# nameif name
```

The *name* is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the **no** form, because that command causes all commands that refer to that name to be deleted. If you name an interface “inside” and you do not set the security level explicitly, then the FWSM sets the security level to 100.

**Step 4** To set the security level, enter the following command:

```
hostname(config-if)# security-level number
```

Where *number* is an integer between 0 (lowest) and 100 (highest). By default, after you name the interface, the FWSM sets the security level to 0.

## Assigning an IP Address to a Bridge Group

A transparent firewall does not participate in IP routing. The only IP configuration required for the FWSM is to set the management IP address for each bridge group. This address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, such as system log messages or communications with AAA servers. You can also use this address for remote management access.

To set the management IP address, perform the following steps:

**Step 1** Identify the bridge group by entering the following command:

```
hostname(config)# interface bvi bridge_group_number
```

**Step 2** Specify the IP address by entering the following command:

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

Do not assign a host address (/32 or 255.255.255.255) to the transparent firewall. Also, do not use other subnets that contain fewer than 3 host addresses (one each for the upstream router, downstream router, and transparent firewall) such as a /30 subnet (255.255.255.252). The FWSM drops all ARP packets to or from the first and last addresses in a subnet. Therefore, if you use a /30 subnet and assign a reserved address from that subnet to the upstream router, then the FWSM drops the ARP request from the downstream router to the upstream router.

The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

The **standby** keyword and address is used for failover. See [Chapter 13, “Configuring Failover,”](#) for more information.

The following example assigns VLANs 300 and 301 to bridge group 1, then sets the management address and standby address of bridge group 1:

```
hostname(config)# interface vlan 300  
hostname(config-if)# nameif inside  
hostname(config-if)# security-level 100  
hostname(config-if)# bridge-group 1  
hostname(config-if)# interface vlan 301  
hostname(config-if)# nameif outside  
hostname(config-if)# security-level 0  
hostname(config-if)# bridge-group 1  
hostname(config-if)# interface bvi 1  
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

## Allowing Communication Between Interfaces on the Same Security Level

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same security interfaces lets you configure more than 101 communicating interfaces. If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).

**Note**

If you enable NAT control, you do not need to configure NAT between same security level interfaces. See the [“NAT and Same Security Level Interfaces” section on page 12-14](#) for more information on NAT and same security level interfaces.

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 to communicate with each other, enter the following command:

```
hostname(config)# same-security-traffic permit inter-interface
```

To disable this setting, use the **no** form of this command.

**Note**

If you use a same-security interface for both the outside and inside interfaces, you might want to enable the **xlate-bypass** command; in some situations, you can exceed the maximum number of xlates using that configuration (see the [“Managed System Resources” section on page A-4](#) for limits). For example, without **xlate-bypass**, the FWSM creates xlates for all connections (even if you do not configure NAT). In a same-security-traffic configuration, the FWSM randomly chooses which same-security interface is the “inside” interface for the sake of creating xlates. If the FWSM considers the outside same-security interface as the “inside” interface, it creates xlates for every Internet host being accessed through it. If there is any application (or a virus) on the internal network that scans thousands of Internet hosts, all entries in the xlate table may be quickly exhausted.

## Turning Off and Turning On Interfaces

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

To disable an interface or reenablen it, perform the following steps:

---

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

```
hostname(config)# interface {vlan number | mapped_name}
```

In multiple context mode, enter the mapped name if one was assigned using the **allocate-interface** command.

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

```
hostname(config)# shutdown
```

**Step 3** To reenablen the interface, enter the following command:

```
hostname(config)# no shutdown
```

---