



CHAPTER 8

Configuring Interfaces

This section contains the following topics:

- [Security Level Overview, page 8-1](#)
- [Configuring Routed Interfaces, page 8-2](#)
- [Configuring Transparent Interfaces and Bridge Groups, page 8-3](#)

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.

The level controls the following behavior:

- Inspection engines—Some inspection engines are dependent on the security level. For some 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 (from a higher level to a lower level).

If you enable communication between 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.

If you enable communication between same security interfaces, you can configure **established** commands for both directions.

Configuring Routed Interfaces

This section describes how to configure routed mode interfaces, and includes the following topics:

- [Adding or Editing a Routed Interface, page 8-2](#)
- [Enabling Same Security Level Communication, page 8-3](#)

Adding or Editing a Routed Interface

In single context mode, you can add any VLAN ID that is assigned to the FWSM by the switch. You cannot add an interface to a context from this dialog box. See the [Security Contexts](#) pane to assign interfaces to contexts.

If you use an interface for failover, do not configure the interface using this procedure; instead, use the [Failover > Setup Tab](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored. After you assign the interface as the failover link or state link, you cannot edit the interface from the Interfaces pane.

To add or edit an interface, perform the following steps:

-
- Step 1** From the Configuration > Interfaces pane, click **Add** or **Edit**.
The Add/Edit Interface dialog box appears with the General tab selected.
- Step 2** If you are adding an interface in single context mode, choose the VLAN ID from the Interface menu.
- Step 3** If the interface is not already enabled, check **Enable Interface**.
The interface is enabled by default. To disable it, uncheck the box.
- Step 4** (Optional) To set this interface as a management-only interface, check **Dedicate this interface to management-only**.
Through traffic is not accepted on a management-only interface.
- Step 5** In the Interface Name field, enter a name up to 48 characters in length.
- Step 6** In the Security level field, enter a level between 0 (lowest) and 100 (highest).
See the [“Security Level Overview”](#) section on page 8-1 for more information.
- Step 7** In the IP Address and Subnet Mask fields, enter the IP address and mask.
- Step 8** (Optional) In the Description field, enter a description for this interface.
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.
- Step 9** (Optional) To set the MTU, click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.
The default is 1500 bytes
-

Enabling Same Security Level Communication

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.

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

You can also enable communication between hosts connected to the same interface.

- To enable interfaces on the same security level to communicate with each other, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.
- To enable communication between hosts connected to the same interface, check **Enable traffic between two or more hosts connected to the same interface**.

Configuring Transparent Interfaces and Bridge Groups

This section describes how to configure transparent mode interfaces and bridge groups, and includes the following topics:

- [Adding or Editing a Bridge Group, page 8-3](#)
- [Adding or Editing a Transparent Interface, page 8-4](#)
- [Enabling Same Security Level Communication, page 8-5](#)

Adding or Editing a Bridge Group

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. 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 syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.



Note All transparent interfaces must belong to a bridge group.

To add or edit a bridge group, perform the following steps:

Step 1 From the Configuration > Interfaces > Bridge Groups tab, click **Add** or **Edit**.

The Add/Edit Bridge Group dialog box appears.

Step 2 In the Bridge Group field, enter the bridge group ID between 1 and 100.

Step 3 In the IP Address field, enter the management IP address.

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 messages or communications with AAA servers. You can also use this address for remote management access.

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

Step 4 In the Subnet Mask field, enter the subnet mask or choose one from the menu.

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. For example, 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.

Step 5 (Optional) In the Description field, enter a description for this bridge group.

Adding or Editing a Transparent Interface

In single mode, you can add any VLAN ID that is assigned to the FWSM by the switch. You cannot add an interface to a context from this dialog box. See the [Security Contexts](#) pane to assign interfaces to contexts.

If you intend to use an interface for failover, do not configure the interface using this procedure; instead, use the [Failover > Setup Tab](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored.

After you assign the interface as the failover link or state link, you cannot edit the interface from the Interfaces pane.

To add or edit an interface, perform the following steps:

Step 1 From the Configuration > Interfaces pane, click **Add** or **Edit**.

The Add/Edit Interface dialog box appears with the General tab selected.

Step 2 If you are adding an interface in single context mode, choose the VLAN ID from the Interface menu.

Step 3 To assign the interface to a bridge group, choose the bridge group ID from the Bridge Group menu.

See the [“Adding or Editing a Bridge Group”](#) section on page 8-3 to view or add a bridge group.

- Step 4** If the interface is not already enabled, check **Enable Interface**.
The interface is enabled by default. To disable it, uncheck the box.
- Step 5** In the Interface Name field, enter a name up to 48 characters in length.
- Step 6** In the Security level field, enter a level between 0 (lowest) and 100 (highest).
See the [“Security Level Overview” section on page 8-1](#) for more information.
- Step 7** In the IP Address and Subnet Mask fields, enter the IP address and mask.
- Step 8** (Optional) In the Description field, enter a description for this interface.
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.
- Step 9** (Optional) To set the MTU, click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.
The default is 1500 bytes
-

Enabling Same Security Level Communication

By default, interfaces on the same security level cannot communicate with each other.



Note

If you enable NAT control, you do not need to configure NAT between 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, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.

