Configuring Interface Parameters

This chapter describes how to configure each interface (physical, redundant, or subinterface) for a name, security level, and IP address.

- For single context mode, the procedures in this chapter continue the interface configuration started in Chapter 5, "Configuring Ethernet Settings, Redundant Interfaces, and Subinterfaces."

- For multiple context mode, the procedures in Chapter 5, "Configuring Ethernet Settings, Redundant Interfaces, and Subinterfaces," are performed in the system execution space, while the procedures in this chapter are performed within each security context.

Note To configure interfaces for the ASA 5505 adaptive security appliance, see Chapter 4, "Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance."

This chapter includes the following sections:

- Security Level Overview, page 7-1
- Configuring Interface Parameters, page 7-2
- Allowing Communication Between Interfaces on the Same Security Level, page 7-7

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 7-7 for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

  If you enable communication for same security interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section on page 7-7), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application 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.

- SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  If you enable communication 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.

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

Configuring Interface Parameters

Before you can complete your configuration and allow traffic through the security appliance, you need to configure an interface name, and for routed mode, an IP address.

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 14, "Configuring Failover." to configure the failover and state links.

This section includes the following topics:

Interface Parameters Overview

This section describes interface parameters and includes the following topics:

Default State of Interfaces

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Security Level

The default security level is 0. If you name an interface "inside" and you do not set the security level explicitly, then the security appliance sets the security level to 100.

> **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 connections using the **clear local-host** command.

Multiple Context Mode Guidelines

For multiple context mode, follow these guidelines:

- Configure the context interfaces from within each context.
- Configure context interfaces that you already assigned to the context in the system configuration. Other interfaces are not available.
- Configure Ethernet settings, redundant interfaces, and subinterfaces in the system configuration. No other configuration is available. The exception is for failover interfaces, which are configured in the system configuration. Do not configure failover interfaces with the procedures in this chapter. See Chapter 14, "Configuring Failover," for more information.

Configuring the Interface

To configure an interface or subinterface, perform the following steps:

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

```
hostname(config)# interface {{redundant number| physical_interface}[.subinterface] |
mapped_name}
hostname(config-if)#
```

The **redundant** *number* argument is the redundant interface ID, such as **redundant 1**.

Append the *subinterface* ID to the physical or redundant interface ID separated by a period (.).

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

The *physical_interface* ID includes the type, slot, and port number as *type* [*slot*/]*port*. The physical interface types include the following:

- **ethernet**
- **gigabitethernet**
- **management** (ASA 5500 only)

For the PIX 500 series security appliance, enter the type followed by the port number, for example, **ethernet 0**.

For the ASA 5500 series adaptive security appliance, enter the type followed by *slot*/*port*, for example, **gigabitethernet 0/1** or **ethernet 0/1**.

✎
Note   For the ASA 5550 adaptive security appliance, for maximum throughput, be sure to balance your traffic over the two interface slots; for example, assign the inside interface to slot 1 and the outside interface to slot 0.

The ASA 5500 management interface is a Fast Ethernet interface designed for management traffic only, and is specified as **management 0/0**. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface (for management purposes) in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode.

For example, enter the following command:

```
hostname(config)# interface gigabitethernet 0/1.1
```

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.

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   (Optional) To set an interface to management-only mode, enter the following command:

```
hostname(config-if)# management-only
```

The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

> ✎
>
> **Note**   Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliance, you can use the Management 0/0 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

Step 5   To set the IP address, enter one of the following commands.

In routed firewall mode, set the IP address for all interfaces. In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole security appliance or context. The exception is for the Management 0/0 management-only interface, which does not pass through traffic. To set the transparent firewall mode whole security appliance or context management IP address, see the "Setting the Management IP Address for a Transparent Firewall" section on page 8-5. To set the IP address of the Management 0/0 interface or subinterface, use one of the following commands.

To set an IPv6 address, see the "Configuring IPv6 on an Interface" section on page 12-3.

For use with failover, you must set the IP address and standby address manually; DHCP and PPPoE are not supported.

- To set the IP address manually, enter the following command:

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

  where the *ip_address* and *mask* arguments set the interface IP address and subnet mask.

  The **standby** *ip_address* argument is used for failover. See Chapter 14, "Configuring Failover," for more information.

- To obtain an IP address from a DHCP server, enter the following command:

  ```
  hostname(config-if)# ip address dhcp [setroute]
  ```

  where the **setroute** keyword lets the security appliance use the default route supplied by the DHCP server.

  Reenter this command to reset the DHCP lease and request a new lease.

  If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

- To obtain an IP address from a PPPoE server, see Chapter 35, "Configuring the PPPoE Client."

  PPPoE is not supported in multiple context mode.

Step 6   (Optional) To assign a private MAC address to this interface, enter the following command:

```
hostname(config-if)# mac-address mac_address [standby mac_address]
```

The *mac_address* is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this command, then it is used regardless of the member interface MAC addresses.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the "How the Security Appliance Classifies Packets" section on page 3-3 for more

information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See the "Automatically Assigning MAC Addresses to Context Interfaces" section on page 6-11 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use the **mac-address** command to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

For use with failover, set the **standby** MAC address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 7   To enable the interface, if it is not already enabled, enter the following command:

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

To disable the interface, enter the **shutdown** command. If you enter the **shutdown** command for a physical or redundant interface, you also shut down all subinterfaces. If you shut down an interface in the system execution space, then that interface is shut down in all contexts that share it, even though the context configurations show the interface as enabled.

The following example configures parameters for the physical interface in single mode:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example configures parameters for a subinterface in single mode:

```
hostname(config)# interface gigabitethernet 0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# mac-address 000C.F142.4CDE standby 020C.F142.4CDE
hostname(config-subif)# no shutdown
```

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet 0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet 0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
hostname/contextA(config)# interface gigabitethernet 0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

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 provides the following benefits:

- You can 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).

- You want traffic to flow freely between all same security interfaces without access lists.

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 17-15 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 so that they can 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.