

Basic Interface Configuration

This chapter includes basic interface configuration including Ethernet settings and Jumbo frame configuration.

Note For multiple context mode, complete all tasks in this section in the system execution space. If you are not already in the system execution space, in the Configuration > Device List pane, double-click **System** under the active device IP address.

Note For the Firepower 2100 in Platform mode and Firepower 4100/9300 chassis, you configure basic interface settings in the FXOS operating system. See the configuration or getting started guide for your chassis for more information.

- About Basic Interface Configuration, on page 1
- Guidelines for Basic Interface Configuration, on page 4
- Default Settings for Basic Interface Configuration, on page 4
- Enable the Physical Interface and Configure Ethernet Parameters, on page 5
- Enable Jumbo Frame Support (ASA Virtual, ISA 3000), on page 7
- Manage the Network Module for the Secure Firewall 3100, on page 8
- Examples for Basic Interfaces, on page 11
- History for Basic Interface Configuration, on page 12

About Basic Interface Configuration

This section describes interface features and special interfaces.

Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For

Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Management Interface

The management interface, depending on your model, is a separate interface just for management traffic.

Management Interface Overview

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management *Slot*/*Port* interface (if available for your model)

You may need to configure management access to the interface according to Management Access.

Management *Slot*/*Port* Interface

The following table shows the Management interfaces per model.

Table 1: Management Interfaces Per Model

Model	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable for Through Traffic	Subinterfaces Allowed
Firepower 1000	—	—	—	**Yes**	**Yes**	**Yes**
Firepower 2100	—	—	—	**Yes**	— **Note:** Technically, you can enable through traffic; however, the throughput of this interface is not adequate for data operations.	**Yes**
Secure Firewall 3100	—	—	—	**Yes**	**Yes**	**Yes**
Firepower 4100/9300	N/A The interface ID depends on the physical mgmt-type interface that you assigned to the ASA logical device	—	—	—	—	**Yes**
ISA 3000	—	—	—	**Yes**	—	—

Model	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable for Through Traffic	Subinterfaces Allowed
ASAv	**Yes**	—	—	—	**Yes**	—

Use Any Interface for Management-Only Traffic

You can use any interface as a dedicated management-only interface by configuring it for management traffic, including an EtherChannel interface.

Management Interface for Transparent Mode

In transparent firewall mode, in addition to the maximum allowed through-traffic interfaces, you can also use the Management interface (either the physical interface, or a subinterface (if supported for your model)) as a separate management-only interface.

You cannot use any other interface types as Management interfaces.

For the Firepower 4100/9300 chassis, the management interface ID depends on the mgmt-type interface that you assigned to the ASA logical device.

Note The management interface is not part of a normal bridge group. Note that for operational purposes, it is part of a non-configurable bridge group.

Management-Only Traffic

The Management interface is for to- and from-the-box traffic only and cannot pass through traffic. In any case, since bridge groups cannot communicate with any other bridge groups, it wouldn't be possible for the Management interface to route to a bridge group or vice versa even if it did support through traffic.

Shared MAC Address Table and Switch Connections

In transparent firewall mode, the Management interface updates the ASA's MAC address table in the same manner as a data interface; therefore you should not connect both a Management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the Management interface from the physically-connected switch, then the ASA updates the MAC address table to use the *Management* interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the ASA will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

Multiple Context Mode

In multiple context mode, you cannot share any interfaces, including the Management interface, across contexts. To provide management per context on supported models, you can create subinterfaces of the Management interface and allocate a Management subinterface to each context. Some models do not allow subinterfaces on the Management interface, so per-context management for these models requires you to connect to a data interface. For the Firepower 4100/9300 chassis, the management interface and its subinterfaces are not recognized as specially-allowed management interfaces within the contexts; you must treat a management subinterface as a data interface in this case and add it to a BVI.

Guidelines for Basic Interface Configuration

Transparent Firewall Mode

For multiple context, transparent mode, each context must use different interfaces; you cannot share an interface across contexts.

Failover

You cannot share a failover or state interface with a data interface.

Additional Guidelines

- Some management-related services are not available until a non-management interface is enabled, and the the ASA achieves a “System Ready” state. The ASA generates the following syslog message when it is in a “System Ready” state:

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

Default Settings for Basic Interface Configuration

This section lists default settings for interfaces if you do not have a factory default configuration.

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.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- VXLAN VNI interfaces—Enabled.
- EtherChannel port-channel interfaces (ISA 3000)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Other models)—Disabled.

Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and on the ASA. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and the ASA.

Default Speed and Duplex

- By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

Default Connector Type

Some models include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default. You can configure the ASA to use the fiber SFP connectors.

Default MAC Addresses

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.

Enable the Physical Interface and Configure Ethernet Parameters

This section describes how to:

- Enable the physical interface
- Set a specific speed and duplex (if available)
- Set Forward Error Correction

This procedure only covers a small subset of Interface settings. Refrain from setting other parameters at this point. For example, you cannot name an interface that you want to use as part of an EtherChannel interface. The exact interface options vary depending on your model and interface type.

Note For the Firepower 4100/9300, you configure basic interface settings in FXOS.

Note For / 1010/ switch ports, see Basic Interface Configuration for Firepower 1010 Switch Ports.

Before you begin

For multiple context mode, complete this procedure in the system execution space. If you are not already in the System configuration mode, in the **Configuration** > **Device List** pane, double-click **System** under the active device IP address.

Procedure

Step 1 Depending on your context mode:

- For single mode, choose the **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** pane.
- For multiple mode in the System execution space, choose the **Configuration** > **Context Management** > **Interfaces** pane.

By default, all physical interfaces are listed.

Step 2 Click a physical interface that you want to configure, and click **Edit**.

The **Edit Interface** dialog box appears.

Note
In single mode, this procedure only covers a subset of the parameters on the **Edit Interface** dialog box. Note that in multiple context mode, before you complete your interface configuration, you need to allocate interfaces to contexts.

Step 3 To enable the interface, check the **Enable Interface** check box.

Step 4 To add a description, enter text in the Description field.

The description can be up to 240 characters on a single line, without carriage returns. 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 5 (Optional) To set the media type, duplex, speed, and enable pause frames for flow control, click **Configure Hardware Properties**.

a) To set the **Duplex**, choose **Full**, **Half**, or **Auto**, depending on the interface type from the drop-down list.

Note
SFP interfaces only support full duplex.

b) To set the **Speed**, choose a value from the drop-down list (varies depending on the model).

For Firepower 1000 and 2100 SFP interfaces, **Negotiate** sets the speed to 1000 Mbps and enables link negotiation for flow-control parameters and remote fault information. For 10 Gbps interfaces, this option sets the speed down to 1000 Mbps. The **Nonegotiate** option disables link negotiation. For other model autonegotiation options, see the **Auto-negotiate** check box on the **Advanced** tab, which lets you enable or disable autonegotiation on any interface 1000 Mbps and higher.

Choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always full, autonegotiation is enabled, and FEC is set to auto. For dual-speed transceivers, the lower speed is used. This option is useful if you later change the network module to a different model, and want the speed to update automatically. Some switches and transceivers don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the ASA to a manual speed and also disable **Auto-negotiate** so the link can come up.

c) To set the **FEC Mode** for 25 Gbps and higher interfaces, choose a value from the drop-down list.

For an EtherChannel member interface, you must configure FEC before you add it to the EtherChannel. If you remove the interface from the EtherChannel, after rebooting, you may need to reconfigure the FEC for the interface.

Some switches don't support auto mode for FEC, especially for larger interfaces. Be sure to either disable FEC or manually configure the setting, depending on the switch support.

The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 2: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC	Network Module Default FEC
25G-SR	cl74-fc	cl108-rs
25G-LR	cl74-fc	cl108-rs
10/25G-CSR	cl74-fc	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate

d) Click **OK** to accept the **Hardware Properties** changes.

Step 6 Click **OK** to accept the **Interface** changes.

Enable Jumbo Frame Support (ASA Virtual, ISA 3000)

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and VLAN header), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the maximum use of other features, such as ACLs. Note that the ASA MTU sets the payload size not including the Layer 2 (14 bytes) and VLAN header (4 bytes), so the maximum MTU is 9198, depending on your model.

This procedure only applies to the ISA 3000 and the ASA Virtual. Other models support jumbo frames by default.

Jumbo frames are not supported on the ASAv5 and ASAv10 with less than 8GB RAM.

Before you begin

- In multiple context mode, set this option in the system execution space.
- Changes in this setting require you to reload the ASA.
- Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9198. In multiple context mode, set the MTU within each context.

- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic, or to increase it in accord with the MTU.

Procedure

Depending on your context mode:

- Multiple mode—To enable jumbo frame support, choose **Configuration > Context Management > Interfaces**, and click the **Enable jumbo frame support** check box.
- Single mode—Setting the MTU larger than 1500 bytes automatically enables jumbo frames. To manually enable or disable this setting, choose **Configuration > Device Setup > Interface Settings > Interfaces**, and click the **Enable jumbo frame support** check box.

Manage the Network Module for the Secure Firewall 3100

If you install a network module before you first power on the firewall, no action is required; the network module is enabled and ready for use.

If you need to make changes to your network module installation after initial bootup, then see the following procedures.

Add a Network Module

To add a network module to a firewall after initial bootup, perform the following steps. Adding a new module requires a reload. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Procedure

Step 1 Install the network module according to the hardware installation guide. You can install the network module while the firewall is powered on.

For clustering or failover, install the network module on all nodes.

Step 2 Reload the firewall; see **Tools > System Reload**.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes with the new module before they can reform the cluster/failover pair.

Step 3 Enable the network module by choosing **Configuration** > **Device Management** > **Advanced** > **EPM**, and unchecking **Disable Netmod**.

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

Step 4 Click **Apply**.

The configuration is applied to the firewall.

Hot Swap the Network Module

You can hot swap a network module for a new module of the same type without having to reload. However, you must shut down the current module to remove it safely. This procedure describes how to shut down the old module, install a new module, and enable it.

For clustering or failover, you cannot disable a network module if the cluster control link/failover link is on the module.

Procedure

Step 1 For clustering or failover, perform the following steps.

- **Clustering**—Ensure the unit you want to perform the hot swap on is a data node (see Change the Control Node); then disable clustering on the node. See Become an Inactive Node or Deactivate a Data Node from the Control Node.

  If the cluster control link is on the network module, you must leave the cluster. See Leave the Cluster. Disabling the network module with an active cluster control link is not allowed.

- **Failover**—Ensure the unit you want to perform the hot swap on is the standby node. See Force Failover.

  If the failover link is on the network module, you must disable failover. See Disable Failover. Disabling the network module with an active failover link is not allowed.

Step 2 Disable the network module by choosing **Configuration** > **Device Management** > **Advanced** > **EPM**, and checking **Disable Netmod**.

Step 3 Click **Apply**.

The configuration is applied to the firewall.

Step 4 Replace the network module according to the hardware installation guide. You can replace the network module while the firewall is powered on.

Step 5 Enable the network module by choosing **Configuration** > **Device Management** > **Advanced** > **EPM**, and unchecking **Disable Netmod**.

Step 6 Click **Apply**.

The configuration is applied to the firewall.

Step 7 For clustering or failover, perform the following steps.

- **Clustering**—Add the node back to the cluster. See Rejoin the Cluster or Add a New Data Node from the Control Node.

- **Failover**—If you disabled failover, then reform failover.

Replace the Network Module with a Different Type

If you replace a network module with a different type, then a reload is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Procedure

Step 1 Disable the network module by choosing **Configuration** > **Device Management** > **Advanced** > **EPM**, and checking **Disable Netmod**.

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

Step 2 Click **Apply**.

The configuration is applied to the firewall. Do not save the configuration; when you reload, the module will be enabled using the saved configuration.

Step 3 Replace the network module according to the hardware installation guide. You can replace the network module while the firewall is powered on.

For clustering or failover, install the network module on all nodes.

Step 4 Reload the firewall; see **Tools > System Reload**.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes with the new module before they can reform the cluster/failover pair.

Step 5 If you saved the configuration before reloading, you will have to reenable the module.

Remove the Network Module

If you want to permanently remove the network module, follow these steps. Removing a network module requires a reload. For clustering or failover, zero downtime is not supported, so make sure to perform this procedure during a maintenance window.

Before you begin

For clustering or failover, make sure the cluster/failover link is not on the network module; you cannot remove the module in this case.

Procedure

Step 1 Disable the network module by choosing **Configuration** > **Device Management** > **Advanced** > **EPM**, and checking **Disable Netmod**.

For clustering or failover, perform this step on the control node/active unit; the module state is replicated to the other nodes.

Step 2 Click **Apply**, and the **Save**.

The configuration is saved to the firewall.

Step 3 Remove the network module according to the hardware installation guide. You can remove the network module while the firewall is powered on.

For clustering or failover, remove the network module on all nodes.

Step 4 Reload the firewall; see **Tools > System Reload**.

For clustering or failover, reload all nodes. Because nodes with different network modules cannot join the cluster/failover pair, you need to reload all nodes without the module before they can reform the cluster/failover pair.

Examples for Basic Interfaces

See the following configuration examples.

Physical Interface Parameters Example

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

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

Multiple Context Mode Example

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

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

History for Basic Interface Configuration

Table 3: History for Interfaces

Feature Name	Releases	Feature Information
Support for hot swapping the network module for the Secure Firewall 3100	9.17(1)	You can add or remove the network module on the Secure Firewall 3100 while the firewall is powered up. To replace a module with another module of the same type, you do not need to reboot. After initial bootup, adding a module, permanently removing a module, or replacing a module with a new type requires a reboot. New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **EPM**
Support for Forward Error Correction for the Secure Firewall 3100	9.17(1)	Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction (FEC). FEC is enabled by default and set to Auto. New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties**
Support for setting the speed based on the SFP for the Secure Firewall 3100	9.17(1)	The Secure Firewall 3100 supports speed detection for interfaces based on the SFP installed. Detect SFP is enabled by default. This option is useful if you later change the network module to a different model, and want the speed to update automatically. New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties**
Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces.	9.17(1)	Secure Firewall 3100 auto-negotiation can be enabled or disabled separately from speed for 1Gigabit and higher interfaces. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Advanced**
Speed auto-negotiation can be disabled on fiber interfaces on the Firepower 1100 and 2100	9.14(1)	You can now configure a Firepower 1100 or 2100 fiber interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified screens: **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties** > **Speed**
Through traffic support on the Management 0/0 interface for the ASA Virtual	9.6(2)	You can now allow through traffic on the Management 0/0 interface on the ASA Virtual. Previously, only the ASA Virtual on Microsoft Azure supported through traffic; now all ASA Virtuals support through traffic. You can optionally configure this interface to be management-only, but it is not configured by default.

Feature Name	Releases	Feature Information
Support for Pause Frames for Flow Control on Gigabit Ethernet Interfaces	8.2(5)/8.4(2)	You can now enable pause (XOFF) frames for flow control for Gigabit Ethernet interfaces on all ASA models. We modified the following screens: (Single Mode) Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > General (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface.
Support for Pause Frames for Flow Control on the ASA 5580 Ten Gigabit Ethernet Interfaces	8.2(2)	You can now enable pause (XOFF) frames for flow control. This feature is also supported on the ASA 5585-X. We modified the following screens: (Single Mode) Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > General (Multiple Mode, System) Configuration > Interfaces > Add/Edit Interface.
Jumbo packet support for the ASA 5580	8.1(1)	The ASA 5580 supports jumbo frames. A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the maximum use of other features, such as ACLs. This feature is also supported on the ASA 5585-X. We modified the following screen: Configuration > Device Setup > Interface Settings > Interfaces > Add/Edit Interface > Advanced.
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 now supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1.
Increased interfaces for the Base license on the ASA 5510	7.2(2)	For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.