Classic Device Management Basics

The following topics describe how to manage Classic devices (ASA with FirePOWER Services/NGIPSv) in the Firepower System:

Requirements and Prerequisites for Classic Device Management

Model Support

Classic models as indicated in the procedures.

Supported Domains

Leaf unless indicated otherwise.

User Roles

- Admin
- Network Admin

Remote Management Configuration (Classic Devices)

For information on configuring remote management for devices that use Classic licenses, see the quick start guide for your device.

Changing the Management Port

Appliances communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

Although Cisco *strongly* recommends that you keep the default setting, you can choose a different port if the management port conflicts with other communications on your network. Usually, changes to the management port are made during installation.

Caution If you change the management port, you must change it for all appliances in your deployment that need to communicate with each other.

You must perform this task in the global domain.

Step 1 Choose **System** > **Configuration**.

Step 2 Click **Management Interfaces**.

Step 3 In the **Shared Settings** section, enter the port number that you want to use in the **Remote Management Port** field.

Step 4 Click **Save**.

What to do next

Repeat this procedure for every appliance in your deployment that must communicate with this appliance.

Interface Configuration Settings

The Interfaces page of the appliance editor displays detailed interface configuration information. The page is composed of the physical hardware view and the interfaces table view, which allow you to drill down to configuration details. You can add and edit interfaces from this page.

The Interfaces Page

The interfaces page lists all the available interfaces you have on a device. The table includes an expandable navigation tree you can use to view all configured interfaces. You can click the arrow icon next to an interface to collapse or expand the interface to hide or view its subcomponents. The interfaces table view also provides summarized information about each interface.

Field	Description
Name	Each interface type is represented by a unique icon that indicates its type and link state (if applicable). You can hover your pointer over the name or the icon to view a tooltip with additional information. The interface icons are described in Interface Icons, on page 3. The icons use a badging convention to indicate the current link state of the interface, which may be one of three states: • **Error** • **Fault** • **Not available** ASA FirePOWER modules do not display link state. Note that disabled interfaces are represented by semi-transparent icons. Interface names, which appear to the right of the icons, are auto-generated with the exception of ASA FirePOWER interfaces, which are user-defined. Note that for ASA FirePOWER interfaces, the system displays only interfaces that are enabled, named, and have link. ASA FirePOWER interfaces display the name of the security context and the name of the interface if there are multiple security contexts. If there is only one security context, the system displays only the name of the interface.
Security Zone	The security zone where the interface is assigned. To add or edit a security zone, click **Edit** ().
Used by (NGIPSv only)	The inline set where the interface is assigned.
MAC Address	For NGIPSv devices, the MAC address is displayed so that you can match the network adapters configured on your device to the interfaces that appear on the Interfaces page.

Interface Icons

Table 1: Interface Icon Types and Descriptions

Icon	Interface Type	Description	See
Passive	Passive	Sensing interface configured to analyze traffic in a passive deployment.	Configuring Passive Interfaces
Inline	Inline	Sensing interface configured to handle traffic in an inline deployment.	Configuring Inline Interfaces
ASA FirePOWER	ASA FirePOWER	Interface configured on an ASA device with the ASA FirePOWER module installed.	Managing Cisco ASA FirePOWER Interfaces, on page 5

Configuring Sensing Interfaces

You can configure the sensing interfaces of a managed device, according to your Firepower deployment, from the Interfaces page of the appliance editor. Note that you can only configure a total of 1024 interfaces on a managed device.

Note The Firepower Management Center does not display ASA interfaces when the ASA FirePOWER is deployed in SPAN port mode.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to configure an interface, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Edit** ( ) next to the interface you want to configure.

Step 4 Use the interface editor to configure the sensing interface:

- Inline — If you want an interface configured to handle traffic in an inline deployment, click **Inline** and proceed as described in Configuring Inline Interfaces.
- Passive — If you want an interface configured to analyze traffic in a passive deployment, click **Passive** and proceed as described in Configuring Passive Interfaces.

Step 5 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Disabling Interfaces

You can disable an interface by setting the interface type to **None**. Disabled interfaces appear grayed out in the interface list.

This procedure applies to NGIPSv.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to disable the interface, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Next to the interface you want to disable, click **Edit** ( ).

Step 4 Click **None**.

Step 5 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Managing Cisco ASA FirePOWER Interfaces

When editing an ASA FirePOWER interface, you can configure only the interface's security zone from the Firepower Management Center.

You fully configure ASA FirePOWER interfaces using the ASA-specific software and CLI. If you edit an ASA FirePOWER and switch from multiple context mode to single context mode (or visa versa), the ASA FirePOWER renames all of its interfaces. You must reconfigure all Firepower System security zones, correlation rules, and related configurations to use the updated ASA FirePOWER interface names. For more information about ASA FirePOWER interface configuration, see the ASA documentation.

Note You cannot change the type of ASA FirePOWER interface, nor can you disable the interface from the Firepower Management Center.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to edit the interface, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Interfaces** if it is not already displaying.

Step 4 Next to the interface you want to edit, click **Edit** ( ).

Step 5 Choose an existing security zone from the **Security Zone** drop-down list, or choose **New** to add a new security zone.

Step 6 Click **Save** to configure the security zone.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

MTU Ranges for NGIPSv

Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Note The system trims 18 bytes from the configured MTU value. Do not set the IPv4 MTU lower than 594 or the IPv6 MTU lower than 1298.

Platform	MTU Range
NGIPSv	576-9018 (all interfaces, inline sets)

Related Topics

About the MTU

Synchronizing Security Zone Object Revisions

When you update a security zone object, the system saves a new revision of the object. As a result, if you have managed devices in the same security zone that have different revisions of the security zone object configured in the interfaces, you may log what appear to be duplicate connections.

If you notice duplicate connection reporting, you can update all managed devices to use the same revision of the object.

This procedure applies to NGIPSv.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to update the security zone selection, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 For each interface logging duplicate connection events, change the **Security Zone** to another zone, click **Save**, then change it back to the desired zone, and click **Save** again.

Step 4 Repeat steps 2 through 3 for each device logging duplicate events. You must edit all devices before you continue.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Caution Do not deploy configuration changes to any device until you edit the zone setting for interfaces on *all* devices you want to sync. You must deploy to all managed devices at the same time.