Classic Device Management Basics

The following topics describe how to manage Classic devices (7000 and 8000 Series/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)

All Devices Except 7000 and 8000 Series

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

7000 and 8000 Series Devices

Configure remote management of a 7000 or 8000 Series device using its local web interface, before you register the device to the FMC.

Before you can manage a Firepower device, you must set up a two-way, SSL-encrypted communication channel between the device and the Firepower Management Center. The appliances use the channel to share configuration and event information. High availability peers also use the channel, which is by default on port 8305/tcp.

To enable communications between two appliances, you must provide a way for the appliances to recognize each other, as follows:

- The hostname or IP address of the appliance with which you are trying to establish communication.

  In NAT environments, even if the other appliance does not have a routable address, you must provide a hostname or an IP address either when you are configuring remote management, or when you are adding the managed appliance.

- A self-generated alphanumeric registration key up to 37 characters in length that identifies the connection.
- An optional unique alphanumeric NAT ID that can help establish communications in a NAT environment.

  The NAT ID *must* be unique among all NAT IDs used to register managed appliances.

Configuring Remote Management on a Managed Device

This procedure applies to 7000 & 8000 Series devices.

Procedure

Step 1 On the web interface for the device you want to manage, choose **System** > **Integration** > **Remote Management**.

Step 2 Click **Remote Management**, if it is not already displaying.

Step 3 Click **Add Manager**.

Step 4 In the **Management Host** field, enter one of the following for the Firepower Management Center that you want to use to manage this appliance:

- The IP address
- The fully qualified domain name or the name that resolves through the local DNS to a valid IP address (that is, the host name)

Caution Use a host name rather than an IP address if your network uses DHCP to assign IP addresses.

In a NAT environment, you do not need to specify an IP address or host name here if you plan to specify it when you add the managed appliance. In this case, the Firepower System uses the NAT ID you will provide later to identify the remote manager on the managed appliance's web interface.

Step 5 In the **Registration Key** field, enter the registration key that you want to use to set up communications between appliances.

Step 6 For NAT environments, in the **Unique NAT ID** field, enter a **unique** alphanumeric NAT ID that you want to use to set up communications between appliances.

Step 7 Click **Save**.

What to do next

- Wait until the appliances confirm that they can communicate with each other and the Pending Registration status appears.
- Add this device to the Firepower Management Center; see Add a Device to the FMC.

Editing Remote Management on a Managed Device

This procedure applies to 7000 & 8000 Series devices.

When editing a remote manager, note that:

- The **Host** field specifies the fully qualified domain name or the name that resolves through the local DNS to a valid IP address (that is, the host name).
- The **Name** field specifies the display name of the managing appliance, which is used only within the context of the Firepower System. Entering a different display name does not change the host name for the managing device.

Procedure

Step 1 On the web interface for the device, choose **System** > **Integration**.

Step 2 Click **Remote Management**, if it is not already displaying.

Step 3 You can:

- Disable remote management — Click the slider next to the manager to enable or disable it. Disabling management blocks the connection between the Firepower Management Center and the device, but does **not** delete the device from the Firepower Management Center. If you no longer want to manage a device, see Delete a Device from the FMC.
- Edit manager information — Click **Edit** () next to the manager you want to modify, modify the **Name** and **Host** fields, and click **Save**.

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.

Procedure

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 Physical Hardware View

The top of the Interfaces page provides a graphical representation of the physical hardware view of a 7000 or 8000 Series device.

Use the physical hardware view to:

- view a network module's type, part number, and serial number
- select an interface in the interfaces table view
- open an interface editor
- view the name of the interface, the type of interface, whether the interface has link, the interface's speed setting, and whether the interface is currently in bypass mode
- view the details about an error or warning

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 6. 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** Logical interfaces have the same link state as their parent physical interface. 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 hybrid and 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. Physical interfaces display the name of the physical interface. Logical interfaces display the name of the physical interface and the assigned VLAN tag. 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	The inline set, virtual switch, or virtual router where the interface is assigned.
MAC Address	The MAC address displayed for the interface when it is enabled for switched and routed features. 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.
IP Addresses (7000/8000 series only)	IP addresses assigned to the interface. Hover your pointer over an IP address to view whether it is active. Inactive IP addresses are also grayed out.

Interface Icons

Table 1: Interface Icon Types and Descriptions

Icon	Interface Type	Description	See
Physical	Physical	Unconfigured physical interface.	Configuring Physical Switched Interfaces or Configuring Physical Routed Interfaces
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
Switched	Switched	Interface configured to switch traffic in a Layer 2 deployment.	Switched Interface Configuration
Routed	Routed	Interface configured to route traffic in a Layer 3 deployment.	Routed Interfaces
Aggregate	Aggregate	Multiple physical interfaces configured as a single logical link.	About Aggregate Interfaces
Aggregate Switched	Aggregate Switched	Multiple physical interfaces configured as a single logical link in a Layer 2 deployment.	Adding Aggregate Switched Interfaces
Aggregate Routed	Aggregate Routed	Multiple physical interfaces configured as a single logical link in a Layer 3 deployment.	Adding Aggregate Routed Interfaces
Hybrid	Hybrid	Logical interface configured to bridge traffic between a virtual router and a virtual switch.	Logical Hybrid Interfaces
ASA FirePOWER	ASA FirePOWER	Interface configured on an ASA device with the ASA FirePOWER module installed.	Managing Cisco ASA FirePOWER Interfaces, on page 10

Using the Physical Hardware View

This task applies to 7000 & 8000 Series devices.

Procedure

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

Step 2 Click edit **Edit** ( ) next to the device you want to manage.

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

Step 3 Use the graphical interface to:

- Choose — If you want to choose an interface, click interface. The system highlights the related entry in the interface table.
- Edit — If you want to open an interface editor, double-click interface.
- View error or warning information — If you want to view the details about an error or warning, hover your cursor over the affected port on the network module.
- View interface information — If you want to view the name of the interface, the type of interface, whether the interface has link, the interface's speed setting, and whether the interface is currently in bypass mode, hover your cursor over the interface.
- View network module information — If you want to view a network module's type, part number, and serial number, hover your cursor over the dark circle in the lower left corner of the network module.

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.

Procedure

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:

- HA Link — If you want an interface configured on each member of a high-availability pair of 7000/8000 series devices to act as a redundant communications channel between the devices; also called a high availability link interface, click **HA Link** and proceed as described in Configuring HA Link Interfaces, on page 8.
- 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.

- Routed — If you want an interface configured to route traffic in a 7000/8000 series Layer 3 deployment, click **Routed** and proceed as described in Routed Interfaces.
- Switched — If you want an interface configured to switch traffic in a 7000/8000 series Layer 2 deployment, click **Switched** and proceed as described in Switched Interface Configuration.

Step 5 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Configuring HA Link Interfaces

After you establish a 7000 or 8000 Series device high-availability pair, you should configure a physical interface as a high availability (HA) link interface. This link acts as a redundant communications channel for sharing health information between the paired devices. When you configure an HA link interface on one device, you automatically configure an interface on the second device. You must configure both HA links on the same broadcast domain.

Dynamic NAT relies on dynamically allocating IP addresses and ports to map to other IP addresses and ports. Without an HA link, these mappings are lost in a failover, causing all translated connections to fail as they are routed through the now-active device in the high-availability pair.

Similarly, 7000 or 8000 Series devices with high-availability state sharing, dynamic NAT, or VPN require an HA link interface.

Procedure

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

Step 2 Next to the peer where you want to configure the HA link 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 configure as a HA link interface, click **Edit** ( ).

Step 4 Click **HA Link**.

Step 5 Check the **Enabled** check box.

If you clear the check box, the system administratively takes down the interface, disabling it.

Step 6 From the **Mode** drop-down list, choose an option to designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to autonegotiate speed and duplex settings.

Step 7 From the **MDI/MDIX** drop-down list, choose an option to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

Normally, MDI/MDIX is set to **Auto-MDIX**, which automatically handles switching between MDI and MDIX to attain link.

Step 8 Enter a maximum transmission unit (MTU) in the **MTU** field.

The range of MTU values can vary depending on the model of the managed device and the interface type. See MTU Ranges for 7000 and 8000 Series Devices and NGIPSv, on page 10 for more information.

Caution 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.

Step 9 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Snort® Restart Scenarios
MTU Ranges for 7000 and 8000 Series Devices and NGIPSv, on page 10

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 and 7000 & 8000 Series devices.

Procedure

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.

Procedure

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 7000 and 8000 Series Devices and 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
7000 & 8000 Series	576-9234 (management interface) 576-10172 (inline sets, passive interface) 576-9922 (all others)
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 and 7000 & 8000 Series devices.

Procedure

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.