Installing a Firepower Managed Device

Firepower System appliances are easily installed on your network as part of a larger Firepower System deployment. You install devices on network segments to inspect traffic and generate intrusion events based on the intrusion policy applied to it. This data is transmitted to a Firepower Management Center, which manages one or more devices to correlate data across your full deployment, and coordinate and respond to threats to your security.

Tip You can use multiple management interfaces to improve performance or to isolate and manage traffic from two different networks. You configure the default management interface (`eth0`) during the initial installation. You can configure additional management interfaces after installation from the user interface. For more information, see *Firepower Management Center Configuration Guide*.

You can pre-configure multiple appliances at one location to be used in different deployment locations. For guidance on pre-configuring, see Preconfiguring Firepower Managed Devices, page E-1.

Note See the ASA documentation for information on installing ASA FirePOWER devices.

Included Items

The following is a list of components that ship with Firepower devices. As you unpack the system and the associated accessories, check that your package contents are complete as follows:

- one appliance
- power cord (two power cords are included with appliances that include redundant power supplies; the power supplies are hot-swappable)
- Category 5e Ethernet straight-through cables: two for a Firepower device
- one rack-mounting kit (required tray and rack-mounting kit available separately for the Firepower 7010, 7020, 7030, and 7050)

Security Considerations

Before you install your appliance, Cisco recommends that you consider the following:

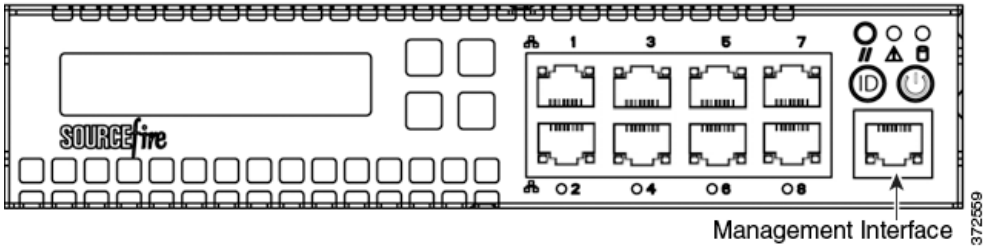
- Locate your appliance in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the appliance.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.
- Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Firepower Management Center Configuration Guide*.

Identifying the Management Interfaces

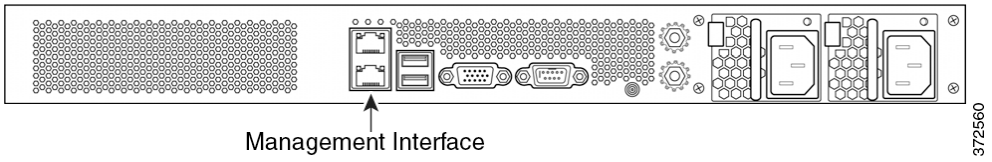
You connect each appliance in your deployment to the network using the management interface. This allows the Firepower Management Center to communicate with and administer the devices it manages. Refer to the correct illustration for your appliance as you follow the installation procedure.

Firepower 7000 Series

The Firepower 7010, 7020, 7030, and 7050 are 1U appliances that are one-half the width of the chassis tray. The following illustration of the front of the chassis indicates the default management interface.

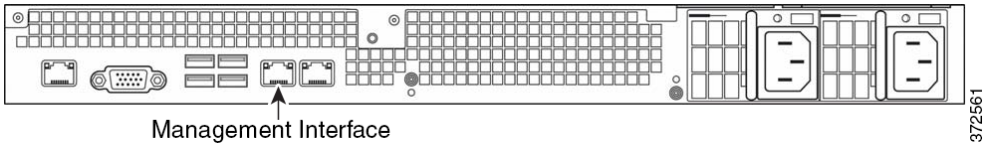


The Firepower 7110/7120, the 7115/7125, and the AMP7150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface.

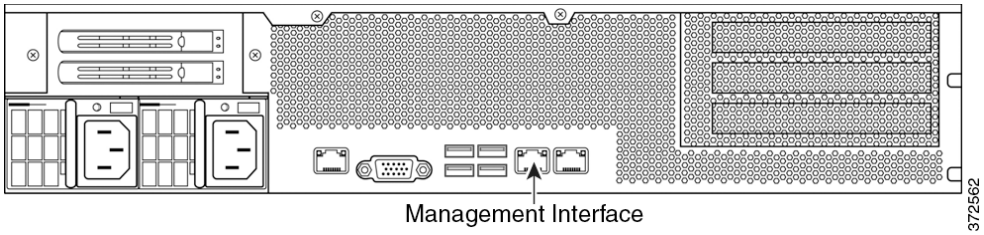


Firepower 8000 Series

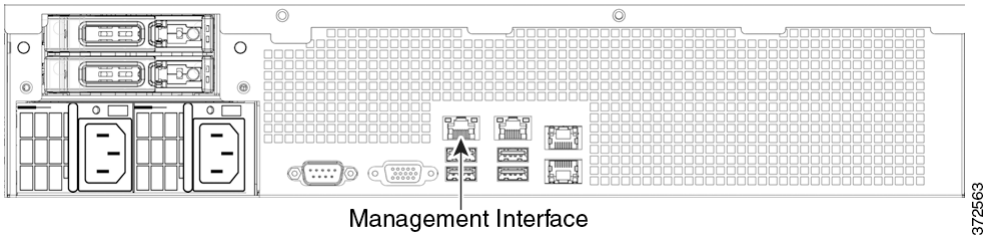
The Firepower 8120, 8130, 8140, and AMP8150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface.



The Firepower 8250 is available as a 2U appliance. The Firepower 8260, 8270, and 8290 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.



The Firepower and AMP 8350 is available as a 2U appliance. The Firepower and AMP 8360, 8370, and 8390 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.



Identifying the Sensing Interfaces

Firepower devices connect to network segments using sensing interfaces. The number of segments each device can monitor depends on the number of sensing interfaces on the device and the type of connection (passive, inline, routed, or switched) that you want to use on the network segment.

The following sections describe the sensing interfaces for each Firepower device:

- To locate the sensing interfaces on the 7000 Series, see Firepower 7000 Series, page 4-3.
- To locate the module slots on the 8000 Series on the Firepower 8000 Series, page 4-7.
- To locate the sensing interfaces on the 8000 Series NetMods, see Firepower 8000 Series Modules, page 4-8.

For information on connection types, see Understanding Sensing Interfaces, page 3-2.

Firepower 7000 Series

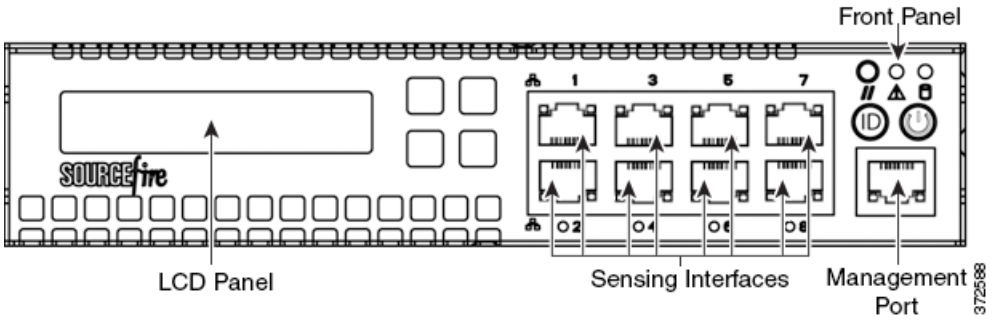
The 7000 Series is available in the following configurations:

- 1U device one-half the width of the rack tray with eight copper interfaces, each with configurable bypass capability.
- 1U device with either eight copper interfaces or eight fiber interfaces, each with configurable bypass capability
- 1U device with four copper interfaces with configurable bypass capability and eight small form-factor pluggable (SFP) ports without bypass capability

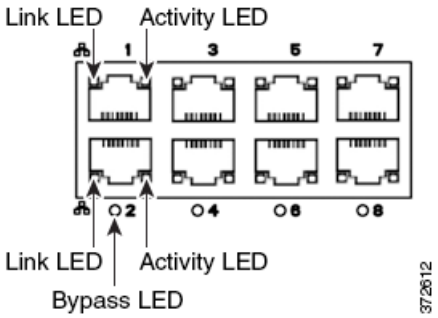
Firepower 7010, 7020, 7030, and 7050

The Firepower 7010, 7020, 7030, and 7050 are delivered with eight copper port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-1 Eight Port 1000BASE-T Copper Configurable Bypass Interfaces



You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.



If you want to take advantage of the device's automatic bypass capability, you must connect two interfaces vertically (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Firepower 7110 and 7120

The Firepower 7110 and 7120 are delivered with eight copper port sensing interfaces, or eight fiber port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-2 Firepower 7110 and 7120 Copper Interfaces

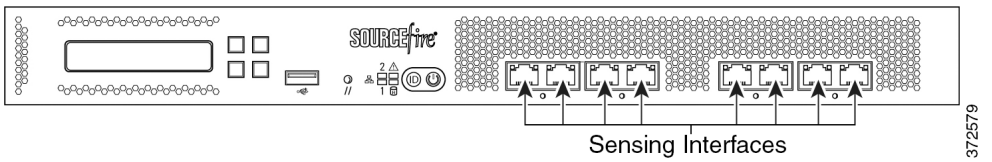
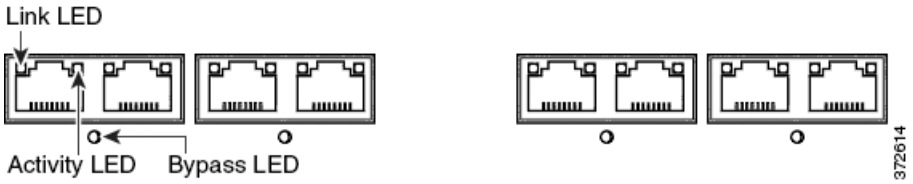


Figure 4-3 Eight-Port 1000BASE-T Copper Interfaces



You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-4 Firepower 7110 and 7120 Fiber Interfaces

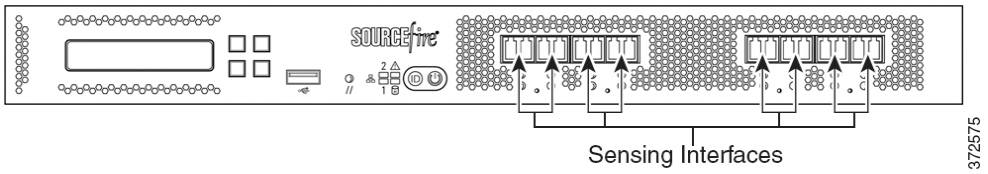


Figure 4-5 Eight-Port 1000BASE-SX Fiber Configurable Bypass

The eight-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

Tip For best performance, use the interface sets consecutively. If you skip any interfaces, you may experience degraded performance.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Firepower 7115, 7125, and AMP7150

The Firepower 7115, 7125, and AMP7150 devices are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-6 Firepower 7115, 7125, and AMP7150 Copper and SFP Interfaces

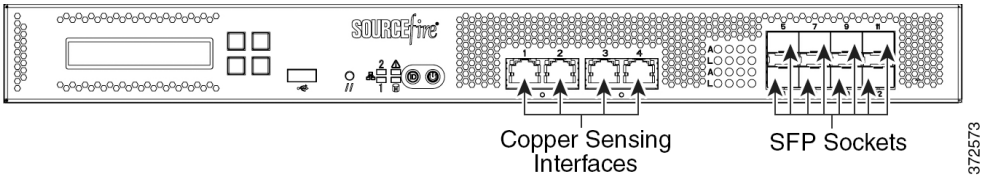
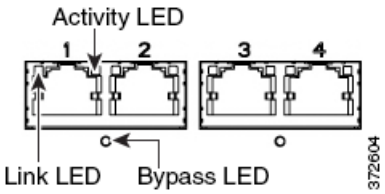


Figure 4-7 Four 1000BASE-T Copper Interfaces



You can use the copper interfaces to passively monitor up to four separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

SFP Interfaces

When you install Cisco SFP transceivers into the SFP sockets, you can passively monitor up to eight separate network segments. You can also use paired interfaces in inline, non-bypass mode to deploy the device as an intrusion detection system on up to four networks.

Cisco SFP transceivers are available in 1G copper, 1G short range fiber, or 1G long range fiber, and are hot-swappable. You can use any combination of copper or fiber transceivers in your device in either passive or inline configuration. Note that SFP transceivers do not have bypass capability and should not be used in intrusion prevention deployments. To ensure compatibility, use only SFP transceivers available from Cisco. See Using SFP Transceivers in 3D71x5 and AMP7150 Devices, page B-1 for more information.

Figure 4-8 Sample SFP Transceivers

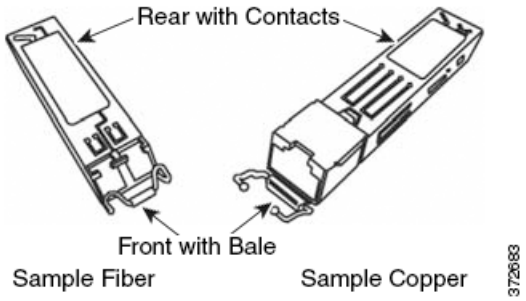
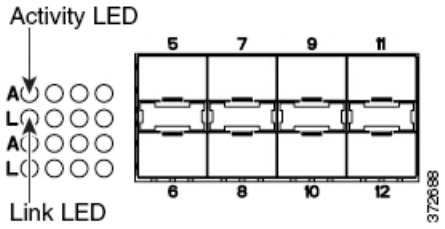


Figure 4-9 SFP Sockets



Firepower 8000 Series

The 8000 Series is available as a 1U device with a 10G network switch or a 2U device with either a 10G or a 40G network switch. This device can be shipped fully assembled, or you can install the network modules (NetMods) that contain the sensing interfaces.

Note If you install a NetMod in an incompatible slot on your device (for example, inserting a 40G NetMod in slots 1 and 4 on a Firepower 8250 or Firepower or AMP 8350) or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface of the managing Firepower Management Center when you attempt to configure the NetMod. Contact Support for assistance.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only)

The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability
- a quad-port 1000BASE-SX fiber interface without bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability

In addition, a stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower and AMP 8360, 8370, 8390 stacked configurations.

Caution Modules are **not** hot-swappable. See Inserting and Removing Firepower 8000 Series Modules, page C-1 for more information.

The following illustrations of the front of the chassis indicates the location of the module slots that contain the sensing interfaces.

Figure 4-10 Firepower 81xx Family Front Chassis View

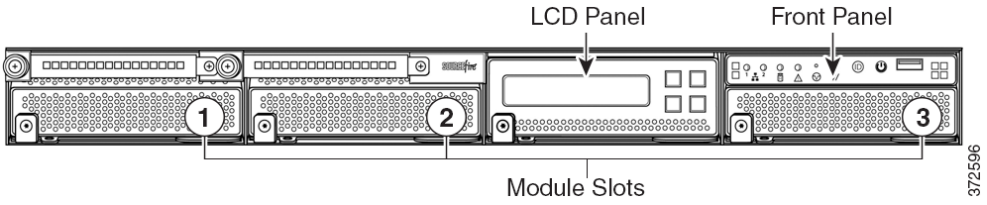
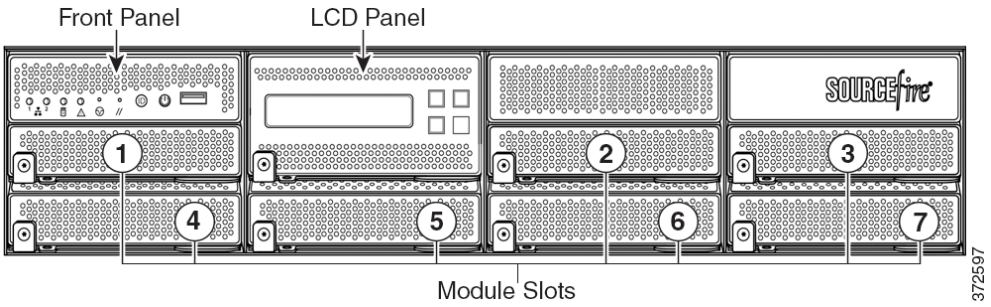


Figure 4-11 Firepower 82xx Family and Firepower and AMP 83xx Family Front Chassis View



Firepower 8000 Series Modules

The Firepower 8000 Series can be delivered with the following modules with configurable bypass capability:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Figure 4-12Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 4-9 for more information.
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Figure 4-13Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 4-9 for more information.
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Figure 4-14Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 4-10 for more information.
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability. See Figure 4-15Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 4-10 for more information.

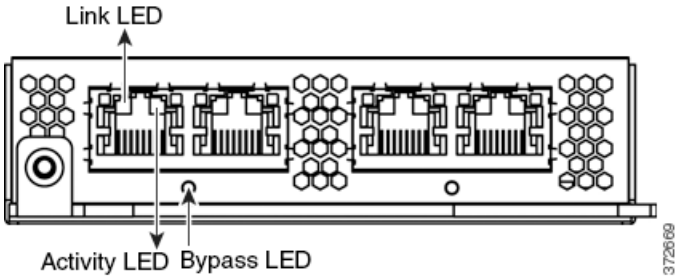
The Firepower 8000 Series can be delivered with the following modules without configurable bypass capability:

- a quad-port 1000BASE-T copper interface without bypass capability. See Figure 4-17Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 4-11 for more information.

- a quad-port 1000BASE-SX fiber interface without bypass capability. See Figure 4-18Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 4-12 for more information.
- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Figure 4-19Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 4-12 for more information.

A stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower 8360, 8370, 8390 stacked configurations. See Firepower 8000 Series Stacking Module, page 4-12 for more information.

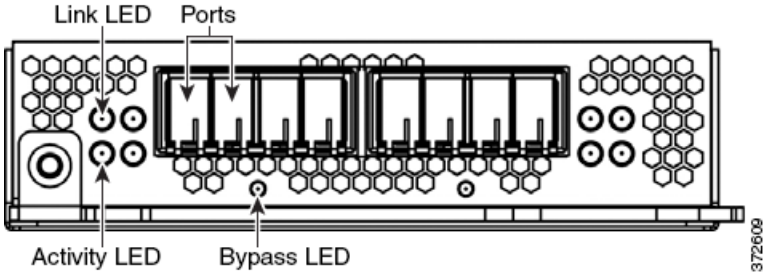
Figure 4-12 Quad-Port 1000BASE-T Copper Configurable Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-13 Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod



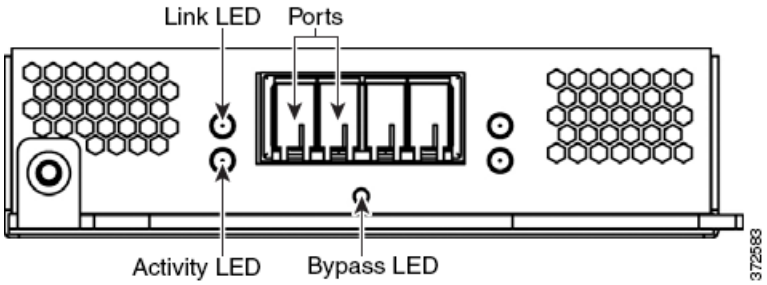
The quad-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use this configuration to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on up to two separate networks.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-14 Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod



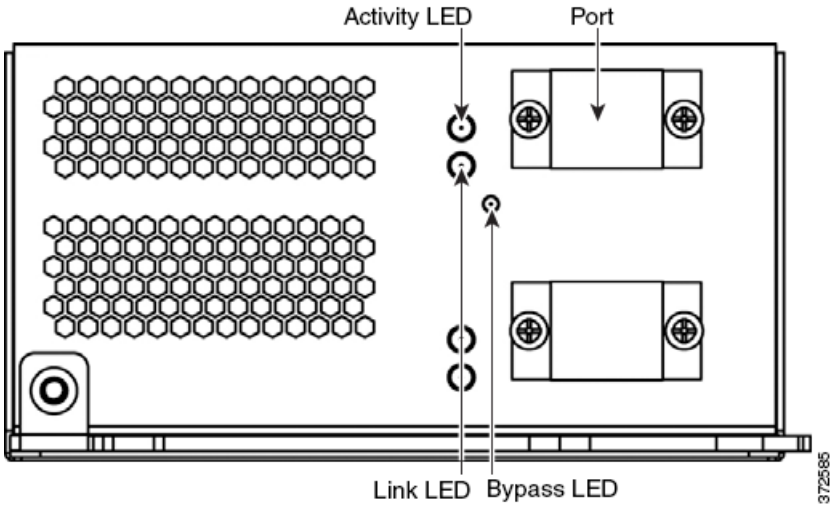
The dual-port 10GBASE fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers. Note that these can be either MMSR or SMLR interfaces.

You can use this configuration to passively monitor up to two separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on a single network.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect two interfaces to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-15 Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod



The dual-port 40GBASE-SR4 fiber configurable bypass configuration uses MPO (Multiple-Fiber Push On) connector optical transceivers.

You can use the 40G NetMod only in the following 8000 Series models:

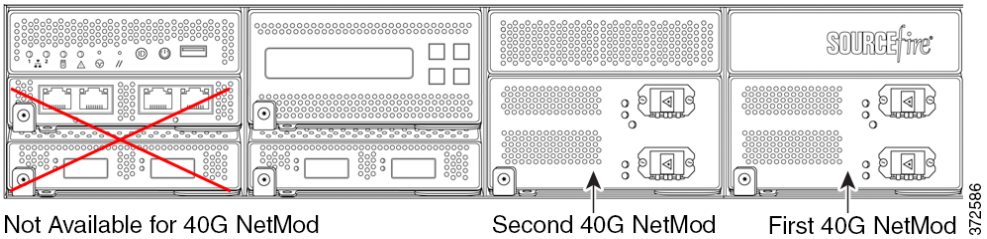
- Firepower 8270 and 8290
- Firepower and AMP 8360, 8370 and 8390
- Firepower 8250 and 8260 (must be 40G-capable)
- Firepower and AMP 8350 (must be 40G-capable)

Caution If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Firepower Management Center web interface displays red. A 40G-capable 8250 displays "8250-40G" on the LCD Panel and a 40G-capable 8350 displays "8350-40G" on the LCD Panel.

You can use this configuration to passively monitor up to two separate network segments. You also can use the paired interface in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on one network.

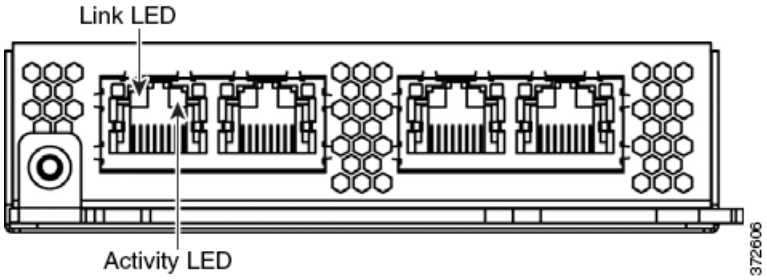
You can use up to two 40G NetMods. Install the first 40G NetMod in slots 3 and 7, and the second in slots 2 and 6. You cannot use a 40G NetMod in slots 1 and 4.

Figure 4-16 40G NetMod Placement



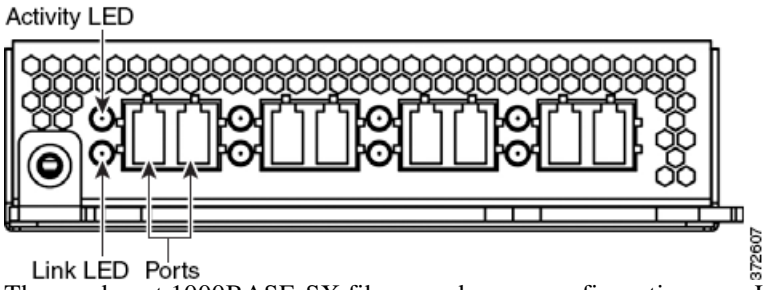
If you want to take advantage of a device's automatic bypass capability, you must use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-17 Quad-Port 1000BASE-T Copper Non-Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Figure 4-18 Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

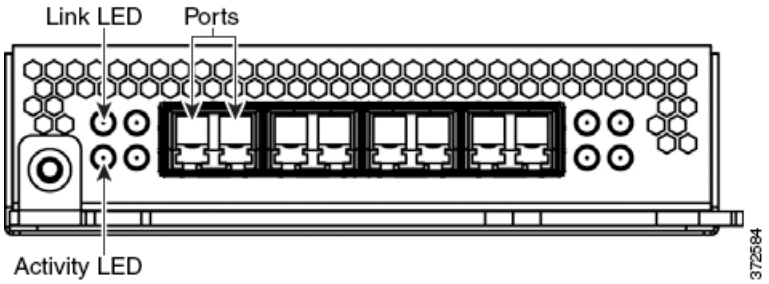


The quad-port 1000BASE-SX fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

Figure 4-19 Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod



The quad-port 10GBASE fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers with either MMSR or SMLR interfaces.

Caution The quad-port 10G BASE non-bypass NetMod contains non-removable small form-factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

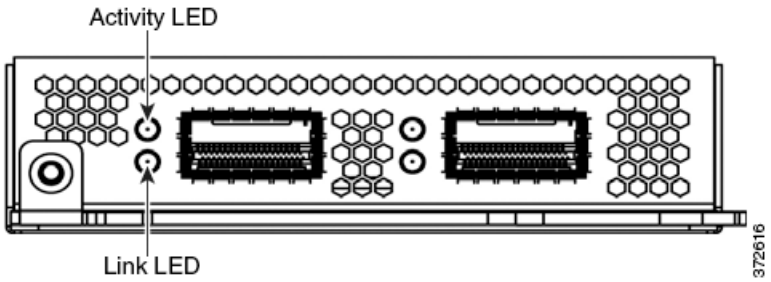
Firepower 8000 Series Stacking Module

A stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the following 8000 Series models:

- Firepower 8140 and 8250
- Firepower and AMP 8350

The stacking module is included in the following 8000 Series stacked configurations:

- Firepower 8260, 8270, and 8290
- Firepower and AMP 8360, 8370, and 8390



The stacking module allows you to combine the resources of two devices, using one as the primary device and one as the secondary. Only the primary device has sensing interfaces. The following devices can use the stacking module:

- The Firepower 8140, 8250, and 8350 can be delivered with the stacking module.
- The Firepower 8260 stacked configuration is delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower and AMP 8360 stacked configurations are delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower 8270 stacked configuration is delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower and AMP 8370 stacked configurations are delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower 8290 stacked configuration is delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.
- The Firepower and AMP 8390 stacked configurations are delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.

For more information on using stacked devices, see Using Devices in a Stacked Configuration.

Using Devices in a Stacked Configuration

You can increase the amount of traffic inspected on network segments by combining the resources of identically configured devices in a stacked configuration. One device is designated as the primary device and is connected to the network segments. All other devices are designated secondary devices, and are used to provide additional resources to the primary device. A Firepower Management Center creates, edits, and manages the stacked configuration.

The primary device contains sensing interfaces and one set of stacking interfaces for each secondary device connected to it. You connect the sensing interfaces on the primary device to the network segments you want to monitor in the same way as a non-stacked device. You connect the stacking interfaces on the primary device to the stacking interfaces on the secondary devices using the stacking cables. Each secondary device is connected directly to the primary device using the stacking interfaces. If a secondary device contains sensing interfaces, they are not used.

You can stack devices in the following configurations:

- two Firepower 8140s

- up to four Firepower 8250s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- up to four Firepower or AMP 8350s
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

For the Firepower 8260 and 8270 devices and Firepower or AMP 8360 and 8370 devices, you can stack additional devices for a total of four devices in the stack.

One device is designated as the primary device and is displayed on the Firepower Management Center's web interface with the primary role. All other devices in the stacked configuration are secondary and displayed in the web interface with the secondary role. You use the combined resources as a single entity except when viewing information from the stacked devices.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140, Firepower 8250, and Firepower or AMP 8350. Connect the secondary devices to the primary device as indicated in the stack cabling diagram.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

After the devices are physically connected to the network segments and to each other, use a Firepower Management Center to establish and manage the stack.

The following sections provide more information on how to connect and manage stacked devices:

- Connecting the Firepower 8140, page 4-14
- Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family, page 4-15
- Using the 8000 Series Stacking Cable, page 4-18
- Managing Stacked Devices, page 4-19

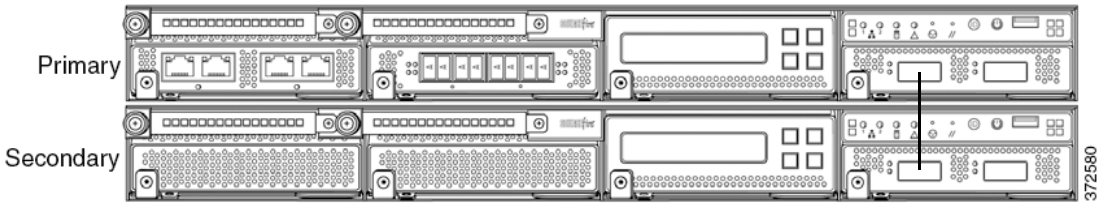
Connecting the Firepower 8140

You can connect two Firepower 8140s in a stacked configuration. You must use one 8000 Series stacking cable to create the physical connection between the primary device and the secondary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 4-18.

Install the devices in your rack so you can easily connect the cable between the stacking modules. You can install the secondary device above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140. Connect the secondary device directly to the primary device.

The following graphic shows a primary device with a secondary device installed below the primary device.



To connect a Firepower 8140 secondary device:

Step 1 Use an 8000 Series stacking cable to connect the left stacking interface on the primary device to the left stacking interface on the secondary device, then use the Firepower Management Center that manages the devices to establish the stacked device relationship in the system. Note that the right stacking interface is not connected. See Managing Stacked Devices, page 4-19.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family

You can connect any of the following configurations:

- up to four 8250s
- up to four Firepower 8350s or four AMP8350s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

You can stack additional devices for a total of four devices in the stack for the following configurations:

- Firepower 8260 and 8270
- Firepower or AMP 8360
- Firepower or AMP 8370

You must use two 8000 Series stacking cables for each secondary device you want to connect to the primary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 4-18.

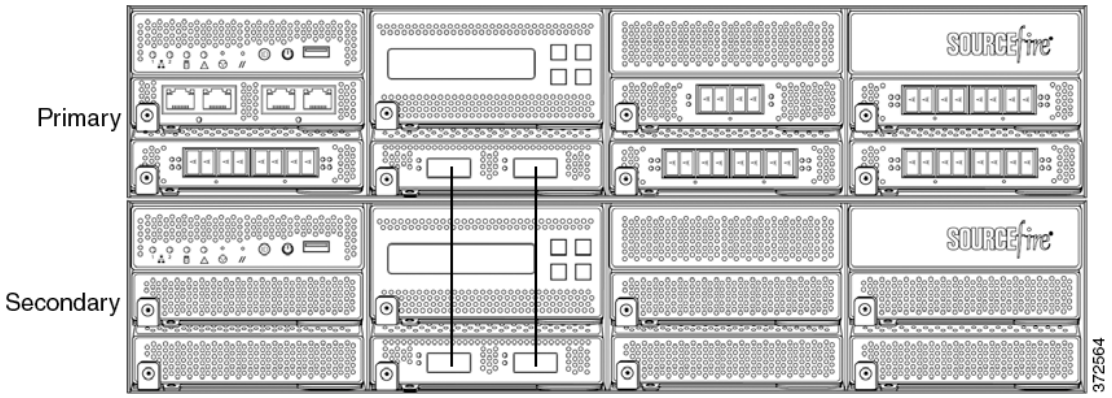
Install the devices in your rack so you can easily connect the cables between the stacking modules. You can install the secondary devices above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8250 or 8350 (Firepower or AMP). Connect each secondary device directly to the primary device as required for the number of secondary devices in the configuration.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

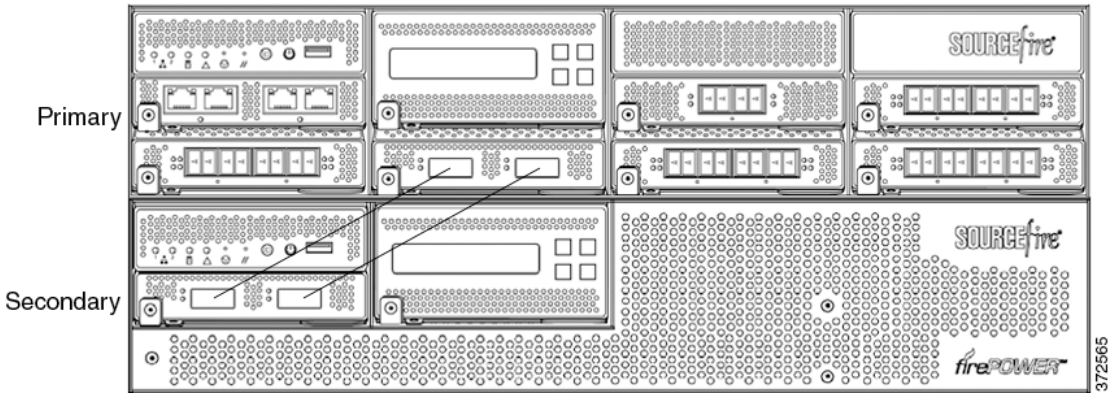
8250 or 8350 Primary Device with One Secondary Device

The following example shows a Firepower 8250 or 8350 (Firepower or AMP) primary device and one secondary device. The secondary device is installed below the primary device. Note that the secondary device contains no sensing interfaces.



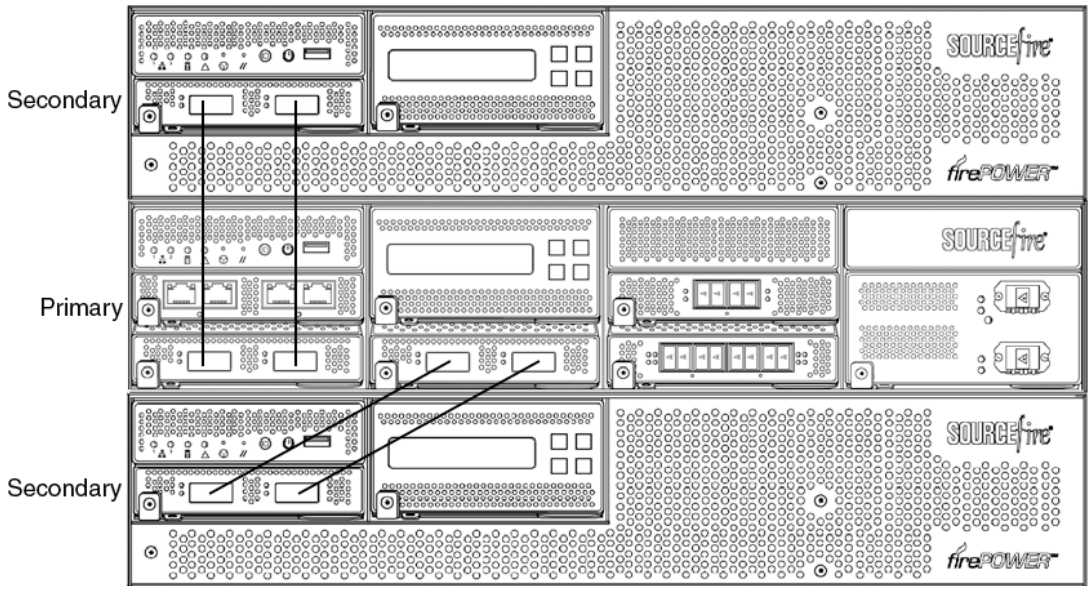
8260 or 8360 Primary Device and One Secondary Device

The following example shows a Firepower 8260 or a 8360 (Firepower or AMP) configuration. The Firepower 8260 includes a 10G-capable 8250 primary device and one dedicated secondary device. The Firepower or AMP 8360 includes a 40G-capable 8350 primary device and one dedicated secondary device. For each configuration (8260 or 8360), the secondary device is installed below the primary device.



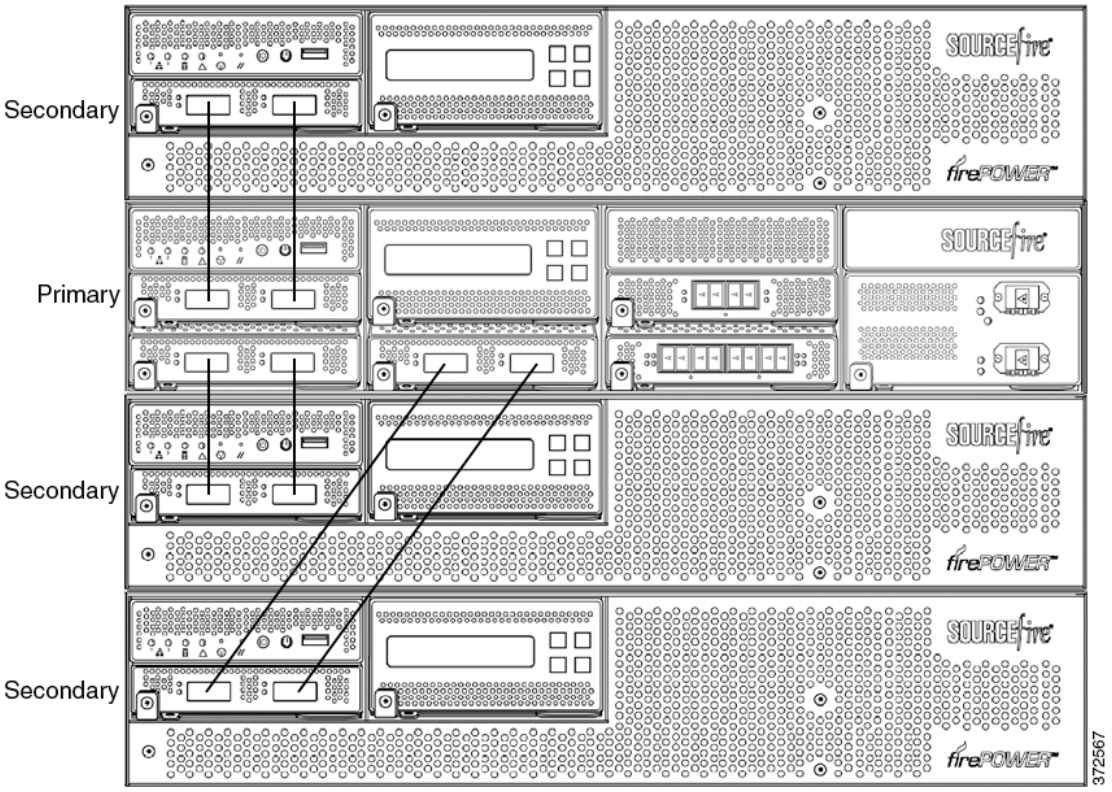
8270 or 8370 Primary Device (40G) and Two Secondary Devices

The following example shows a Firepower 8270 or a 8370 (Firepower or AMP) configuration. The Firepower 8270 includes a 40G-capable 8250 primary device and two dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8270 or 8370), one secondary device is installed above the primary device and the other is installed below the primary device.



8290 or 8390 Primary Device (40G) and Three Secondary Devices

The following example shows a Firepower 8290 or a 8390 (Firepower or AMP) configuration. The Firepower 8290 includes a 40G-capable 8250 primary device and three dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8290 or 8390), one secondary device is installed above the primary device and two secondary devices are installed below the primary device.



To connect a 8250 or a 8350 secondary device:

Step 1 Use an 8000 Series stacking cable to connect the left interface on the stacking module on the primary device to the left interface on the stacking module on the secondary device.

Step 2 Use a second 8000 Series stacking cable to connect the right interface on the stacking module on the primary device to the right interface on the stacking module on the secondary device.

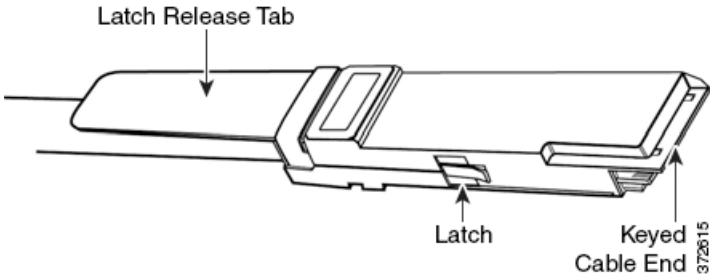
Step 3 Repeat steps 1 and 2 for each secondary device you want to connect.

Step 4 Use the Firepower Management Center that manages the devices to establish the stacked device relationship and manage their joint resources. See Managing Stacked Devices, page 4-19.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Using the 8000 Series Stacking Cable

The 8000 Series stacking cable has identically-keyed ends, each with a latch to secure the cable in the device and a latch release tab.



Use 8000 Series stacking cables to create the physical connection between the primary device and each secondary device as required for each device configuration:

- the Firepower 8250, 8260, 8270, and 8290 require two cables per connection
- the Firepower or AMP 8350, 8360, 8370, and 8390 require two cables per connection
- the Firepower 8140 requires one cable

Devices do not need to be powered down to insert or remove the stacking cable.

Caution Use only the Cisco 8000 Series stacking cable when cabling your devices. Using unsupported cables can create unforeseen errors.

Use the Firepower Management Center to manage the stacked devices after you have physically connected the devices.

To insert an 8000 Series stacking cable:

Step 1 To insert the cable, hold the cable end with release tab facing up, then insert the keyed end into the port on the stacking module until you hear the latch click into place.

To remove an 8000 Series stacking cable:

Step 1 To remove the cable, pull on the release tab to release the latch, then remove the cable end.

Managing Stacked Devices

A Firepower Management Center establishes the stacked relationship between the devices, controls the interface sets of the primary device, and manages the combined resources in the stack. You cannot manage interface sets on the local web interface of a stacked device.

After the stacked relationship is established, each device inspects traffic separately using a single, shared detection configuration. If the primary device fails, traffic is handled according to the configuration of the primary device (that is, as if the stacked relationship did not exist). If the secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to the failed secondary device where the traffic is dropped.

For information on establishing and managing stacked devices, see Managing Stacked Devices in the *Firepower Management Center Configuration Guide*.

Rack-Mounting a Firepower Device

You can rack-mount all Firepower devices (with purchase of a 1U mounting kit for Firepower 7010, 7020, 7030, and 7050). When you install an appliance, you must also make sure that you can access its console. To access the console for initial setup, connect to the appliance in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to a Firepower device, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch.

Caution Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

Ethernet Connection to Management Interface

Configure a local computer, which must not be connected to the Internet, with the following network settings:

- IP address: `192.168.45.2`
- netmask: `255.255.255.0`
- default gateway: `192.168.45.1`

Using an Ethernet cable, connect the network interface on the local computer to the management interface on the appliance. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are as follows:

- 9600 baud
- 8 data bits
- no parity checking
- 1 stop bit
- no flow control.

Note that the management interface is preconfigured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.

After initial setup, you can access the console in the following additional ways:

Serial Connection/Laptop

You can connect a computer to a Firepower device using the appliance's serial port. Connect the appropriate rollover serial cable (also known as a NULL modem cable or Cisco console cable) at any time, then configure the remote management console to redirect the default VGA output to the serial port. To interact with the appliance, use terminal emulation software as described above.

A serial port may have an RJ-45 connection or a DB-9 connection, depending on the appliance. See the following table for connectors by appliance.

Table 4-1 Serial Connectors by Model

Firepower Appliance	Connectors
70xx Family	RJ-45

Table 4-1 Serial Connectors by Model

Firepower Appliance	Connectors
71xx Family	DB-9 (female)
8000 Series	RJ-45

After you connect the appropriate rollover cable to your device, redirect the console output as described in Redirecting Console Output, page 4-22. To locate the serial port for each appliance, use the diagrams in Hardware Specifications, page 7-1.

Lights-Out Management Using Serial over LAN

The LOM feature allows you to perform a limited set of actions on a Firepower Management Center or Firepower device using a SOL connection. If you need to restore a LOM-capable appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. For more information, see Setting Up Lights-Out Management, page 8-15.

Note You can use Lights-Out Management on the default (`eth0`) management interface only.

To use LOM to restore the appliance to factory settings, do **not** delete network settings. Deleting the network settings also drops the LOM connection. For more information, see Restoring a Firepower System Appliance to Factory Defaults, page 8-1.

To install the appliance:

Step 1 Mount the appliance in your rack using the mounting kit and its supplied instructions.

Step 2 Connect to the appliance using either a keyboard and monitor or Ethernet connection.

Step 3 If you are using a keyboard and monitor to set up the appliance, use an Ethernet cable now to connect the management interface to a protected network segment.

If you plan to perform the initial setup process by connecting a computer directly to the appliance's management interface, you will connect the management interface to the protected network when you finish setup.

Step 4 For a Firepower device, connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces:

- Copper Sensing Interfaces: If your device includes copper sensing interfaces, make sure you use the appropriate cables to connect them to your network; see Cabling Inline Deployments on Copper Interfaces, page 3-5.
- Fiber Adapter Card: For devices with a fiber adapter card, connect the LC connectors on the optional multimode fiber cable to two ports on the adapter card in any order. Connect the SC plug to the network segment you want to analyze.
- Fiber Tap: If you are deploying the device with an optional fiber optic tap, connect the SC plug on the optional multimode fiber cable to the "analyzer" port on the tap. Connect the tap to the network segment you want to analyze.

- Copper Tap: If you are deploying the device with an optional copper tap, connect the A and B ports on the left of the tap to the network segment you want to analyze. Connect the A and B ports on the right of the tap (the "analyzer" ports) to two copper ports on the adapter card.

For more information about options for deploying the managed device, see Deploying Firepower Managed Devices, page 3-1.

Note that if you are deploying a device with bypass interfaces, you are taking advantage of your device's ability to maintain network connectivity even if the device fails. See Testing an Inline Bypass Interface Installation, page 4-24 for information on installation and latency testing.

Step 5 Attach the power cord to the appliance and plug into a power source.

If your appliance has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources.

Step 6 Turn on the appliance.

If you are using a direct Ethernet connection to set up the appliance, confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance. If the management interface and network interface LEDs are not lit, try using a crossover cable. For more information, see Cabling Inline Deployments on Copper Interfaces, page 3-5.

What To Do Next

- Continue with the next chapter, Setting Up Firepower Managed Devices, page 5-1.

Redirecting Console Output

By default, Firepower devices direct initialization status, or *init*, messages to the VGA port. If you restore an appliance to factory defaults and delete its license and network settings, the restore utility also resets the console output to VGA. If you want to use the physical serial port or SOL to access the console, Cisco recommends you redirect console output to the serial port after you complete the initial setup.

To redirect console output using the shell, you run a script from the appliance's shell. Note that while all Firepower devices support LOM, 7000 Series devices do not support LOM and physical serial access at same time. However, the console setting is the same regardless of which access method you want to use.

Using the Shell

You can use the shell to redirect the console output.

To redirect the console output using the shell:

Access: Admin

Step 1 Using your keyboard/monitor or serial connection, log into the appliance's shell using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

On a Firepower device, you must type `expert` to display the shell prompt.

The prompt for the appliance appears.

Step 2 At the prompt, set the console output by typing one of the following commands:

- To access the appliance using the VGA port:

```
sudo /usr/local/sf/bin/configure_console.sh vga
```

- To access the appliance using the physical serial port:

```
sudo /usr/local/sf/bin/configure_console.sh serial
```

- To access the appliance using LOM via SOL:

```
sudo /usr/local/sf/bin/configure_console.sh sol
```

Step 3 To implement your changes, reboot the appliance by typing `sudo reboot`.

The appliance reboots.

Using the Web Interface

You can also redirect console output through the web interface.

To redirect the console output using the web interface:

Access: Admin

Step 1 Select **System > Configuration.**

Step 2 Select **Console Configuration.**

Step 3 Select a remote console access option:

- Select **VGA** to use the appliance's VGA port. This is the default option.
- Select **Physical Serial Port** to use the appliance's serial port, or to use LOM/SOL on a Firepower 7050 or 8000 Series device.

  The LOM settings appear.
- Select **Lights-Out Management** to use LOM/SOL on a 7000 Series device (except the Firepower 7050).

  On these devices, you cannot use SOL and a regular serial connection at the same time. LOM settings appear.

Step 4 To configure LOM via SOL, enter the appropriate settings:

- **DHCP Configuration** for the appliance (**DHCP** or **Static**).
- **IP Address** to be used for LOM. The LOM IP address must be different from the management interface IP address of the appliance.
- **Netmask** for the appliance.
- **Default Gateway** for the appliance.

Step 5 Click **Save**.

Remote console configuration for the appliance is saved. If you configured Lights-Out Management, you must enable it for at least one user; see Enabling LOM and LOM Users, page 8-16.

Testing an Inline Bypass Interface Installation

Managed devices with bypass interfaces provide the ability to maintain network connectivity even when the device is powered off or inoperative. It is important to ensure that you properly install these devices and quantify any latency introduced by their installation.

Note Your switch's spanning tree discovery protocol can cause a 30-second traffic delay. Cisco recommends that you disable the spanning tree during the following procedure.

The following procedure, applicable only to copper interfaces, describes how to test the installation and ping latency of an inline bypass interface. You will need to connect to the network to run ping tests and connect to the managed device console.

Before You Begin

- Ensure that the interface set type for the Firepower device is configured for inline bypass mode. See Configuring Inline Sets in the *Firepower Management Center Configuration Guide* for instructions on configuring an interface set for inline bypass mode.

To test a device with inline bypass interface installation:

Access: Admin

Step 1 Set all interfaces on the switch, the firewall, and the device sensing interfaces to auto-negotiate.

Note Firepower System devices require auto-negotiate when using auto-MDIX on the device.

Step 2 Power off the device and disconnect all network cables.

Reconnect the device and ensure you have the proper network connections. Check cabling instructions for crossover versus straight-through from the device to the switches and firewalls, see Cabling Inline Deployments on Copper Interfaces, page 3-5.

Step 3 With the device powered off, ensure that you can ping from the firewall through the device to the switch.

If the ping fails, correct the network cabling.

Step 4 Run a continuous ping until you complete step 9.

Step 5 Power the device back on.

Step 6 Using your keyboard/monitor or serial connection, log into the device using an account with Administrator privileges. The password is the same as the password for the device's web interface.

The prompt for the device appears.

Step 7 Shut down the device by typing `system shutdown`.

You can also shut down the device using its web interface; see the Managing Devices chapter in the *Firepower Management Center Configuration Guide.* As most devices power off, they emit an audible click sound. The click is the sound of relays switching and the device going into hardware bypass.

Step 8 Wait 30 seconds.

Verify that your ping traffic resumes.

Step 9 Power the device back on, and verify that your ping traffic continues to pass.

Step 10 For Firepower devices that support tap mode, you can test and record ping latency results under the following sets of conditions:

- device powered off
- device powered on, policy with no rules applied, inline intrusion policy protection mode
- device powered on, policy with no rules applied, inline intrusion policy protection tap mode
- device powered on, policy with tuned rules applied, inline intrusion policy protection mode

Ensure that the latency periods are acceptable for your installation. For information on resolving excessive latency problems, see Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding in the *Firepower Management Center Configuration Guide*.