Deploying on a Management Network

The Firepower System can be deployed to accommodate the needs of each unique network architecture. The Management Center provides a centralized management console and database repository for the Firepower System. Devices are installed on network segments to collect traffic connections for analysis.

Management Centers use a management interface to connect to a *trusted management network* (that is, a secure internal network not exposed external traffic). Devices connect to a Management Center using a management interface.

Devices then connect to an external network using sensing interfaces to monitor traffic. For more information on how to use sensing interfaces in your deployment, see Deploying Firepower Managed Devices in the *Firepower 7000 and 8000 Series Installation Guide*.

Note See the ASA documentation for more information on deployment scenarios for ASA FirePOWER devices.

Management Deployment Considerations

Your management deployment decisions are based on a variety of factors. Answering these questions can help you understand your deployment options to configure the most efficient and effective system:

- Will you use the default single management interface to connect your device to your Management Center? Will you enable additional management interfaces to improve performance, or to isolate traffic received on the Management Center from different networks? See Understanding Management Interfaces, page 4-2 for more information.
- Do you want to enable traffic channels to create two connections between the Management Center and the managed device to improve performance? Do you want to use multiple management interfaces to further increase throughput capacity between the Management Center and the managed device? See Deploying with Traffic Channels, page 4-3 for more information.
- Do you want to use one Management Center to manage and isolate traffic from devices on different networks? See Deploying with Network Routes, page 4-4 for more information.
- Are you deploying your management interfaces in a protected environment? Is appliance access restricted to specific workstation IP addresses? Security Considerations, page 4-5 describes considerations for deploying your management interfaces securely.
- Are you deploying 8000 Series devices? See Special Case: Connecting 8000 Series Devices, page 4-5 for more information.

Understanding Management Interfaces

Management interfaces provide the means of communication between the Management Center and all devices it manages. Maintaining good traffic control between the appliances is essential to the success of your deployment.

On Management Centers and Firepower devices, you can enable the management interface on the Management Center, device, or both, to sort traffic between the appliances into two separate traffic channels. The *management traffic channel* carries all internal traffic (that is, inter-device traffic specific to the management of the appliance and the system), and the *event traffic channel* carries all event traffic (that is, high volume event traffic, such as intrusion and malware events). Splitting traffic into two channels creates two connection points between the appliances which increases throughput, thus improving performance. You can also enable *multiple management interfaces* to provide still greater throughput between appliances, or to manage and isolate traffic between devices on different networks.

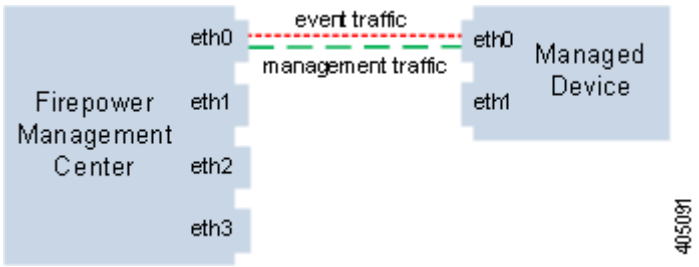
After you register the device to the Management Center, you can change the default configuration to enable traffic channels and multiple management interfaces using the web interface on each appliance. For configuration information, see Configuring Appliance Settings in the *Firepower Management Center Configuration Guide*.

Management interfaces are often located on the back of the appliance. See Identifying the Management Interfaces, page 3-2 for more information.

Single Management Interface

When you register your device to a Management Center, you establish a single communication channel that carries all traffic between the management interface on the Management Center and the management interface on the device.

The following graphic shows the default single communication channel. One interface carries one communication channel that contains both management and event traffic.



Multiple Management Interfaces

You can enable and configure multiple management interfaces, each with a specific IPv4 or IPv6 address and, optionally, a hostname, to provide greater traffic throughput by sending each traffic channel to a different management interface. Configure a smaller interface to carry the lighter management traffic load, and a larger interface to carry the heavier event traffic load. You can register devices to separate management interfaces and configure both traffic channels for the same interface, or use a dedicated management interface to carry the event traffic channels for all devices managed by the Management Center.

You can also create a route from a specific management interface on your Management Center to a different network, allowing your Management Center to isolate and manage device traffic on one network separately from device traffic on another network.

Additional management interfaces function the same as the default management interface with the following exceptions:

- You can configure DHCP on the default (`eth0`) management interface only. Additional (`eth1` and so on) interfaces require unique static IP addresses and hostnames. Cisco recommends that you do not set up DNS entries for additional management interfaces but instead register Management Centers and devices by IP addresses only for these interfaces.
- You must configure both traffic channels to use the same management interface when you use a non-default management interface to connect your Management Center and managed device and those appliances are separated by a NAT device.
- You can use Lights-Out Management on the default management interface only.
- On the 70xx Family, you can separate traffic into two channels and configure those channels to send traffic to one or more management interfaces on the Management Center. However, because the 70xx Family contains only one management interface, the device receives traffic sent from the Management Center on only one management interface.

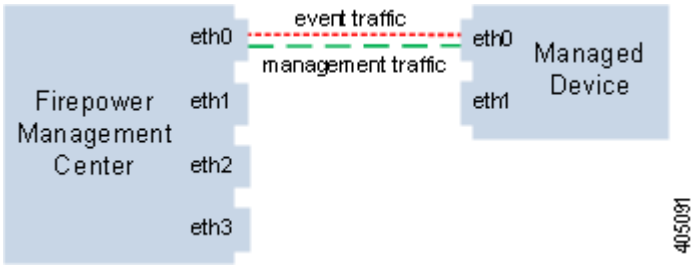
Deployment Options

You can manage traffic flow using traffic channels to improve performance on your system using one or more management interfaces. In addition, you can create a route to a different network using a specific management interface on the Management Center and its managed device, allowing you to isolate traffic between devices on different networks. For more information, see the following sections:

Deploying with Traffic Channels

When you use two traffic channels on one management interface, you create two connections between the Management Center and the managed device. One channel carries management traffic and one carries event traffic, separately and on the same interface.

The following example shows the communication channel with two separate traffic channels on the same interface.

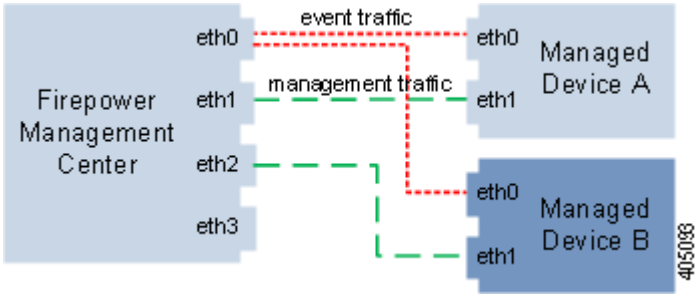


When you use multiple management interfaces, you can improve your performance by dividing the traffic channels over two management interfaces, thus increasing the traffic flow by adding the capacity of both interfaces. One interface carries the management traffic channel and the other carries the event traffic channel. If the event network goes down, then event traffic reverts to the regular management interface. The device uses a separate event interface when possible, but the management interface is always the backup.

The following graphic shows the management traffic channel and the event traffic channel over two management interfaces.

You can use a dedicated management interface to carry only event traffic from multiple devices. In this configuration, each device is registered to a different management interface to carry the management traffic channel, and one management interface on the Management Center carries all event traffic channels from all devices. If the event network goes down, then event traffic reverts to the regular management interface. Note that because event traffic for all devices is carried on the same interface, traffic is not isolated between networks.

The following graphic shows two devices using different management channel traffic interfaces sharing the same dedicated interface for event traffic channels.



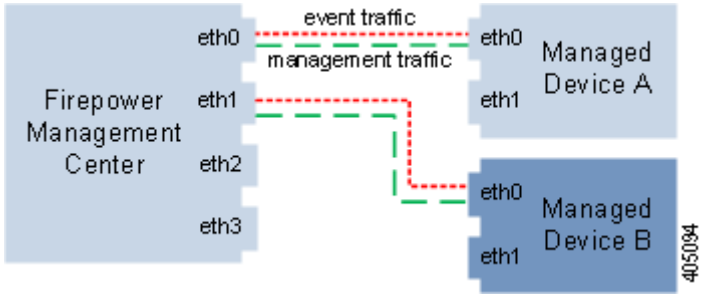
Deploying with Network Routes

You can create a route from a specific management interface on your Management Center to a different network. When you register a device from that network to the specified management interface on the Management Center, you provide an isolated connection between the Management Center and the device on a different network. Configure both traffic channels to use the same management interface to ensure that traffic from that device remains isolated from device traffic on other networks. Because the routed interface is isolated from all other interfaces on the Management Center, if the routed management interface fails, the connection is lost.

Tip You must register a device to the static IP address of any management interface other than the default (`eth0`) management interface. DHCP is supported only on the default management interface.

After you install your Management Center, you configure multiple management interfaces using the web interface. See Configuring Appliance Settings in the *Firepower Management Center Configuration Guide* for more information.

The following graphic shows two devices isolating network traffic by using separate management interfaces for all traffic. You can add more management interfaces to configure separate management and event traffic channel interfaces for each device.



Security Considerations

To deploy your management interfaces in a secure environment, Cisco recommends that you consider the following:

- Always connect the management interface to a trusted 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*.

Special Case: Connecting 8000 Series Devices

Supported Devices: 8000 Series

When you register an 8000 Series device to your Management Center, you must either auto-negotiate on both sides of the connection, or set both sides to the same static speed to ensure a stable network link. 8000 Series devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection.