



Interfaces

The following topics explain how to configure the interfaces on your FTD device.

- [About FTD Interfaces, on page 1](#)
- [Guidelines and Limitations for Interfaces, on page 5](#)
- [Configuring Interfaces, on page 7](#)
- [Monitoring Interfaces, on page 18](#)
- [Examples for Interfaces, on page 19](#)

About FTD Interfaces

The FTD device includes data interfaces as well as a management/diagnostic interface. The following topics explain the limitations of configuring interfaces through Firepower Device Manager as well as other interface management concepts.

Data Interfaces

You can configure the following types of interfaces:

Routed

Each Layer 3 routed interface (or subinterface) requires an IP address on a unique subnet. You would typically attach these interfaces to switches, a port on another router, or to an ISP/WAN gateway.

You can assign a static address, or you can obtain one from a DHCP server. However, if the DHCP server provides an address on the same subnet as a statically-defined interface on the device, the system will disable the DHCP interface. If an interface that uses DHCP to get an address stops passing traffic, check whether the address overlaps the subnet for another interface on the device.

Bridged

A bridge group is a group of interfaces that the Firepower Threat Defense device bridges instead of routes. Bridged interfaces belong to a bridge group, and all interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network.

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the Internet.

One use for a bridge group in routed mode is to use extra interfaces on the Firepower Threat Defense device instead of an external switch. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.

You can configure both IPv6 and IPv4 addresses on a routed interface or BVI. Make sure you configure a default route for both IPv4 and IPv6. You do not configure addresses on bridge group member interfaces.

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- **Global**—The global address is a public address that you can use on the public network. For a bridge group, you configure the global address on the Bridge Virtual Interface (BVI), not on each member interface. You cannot specify any of the following as a global address.
 - Internally reserved IPv6 addresses: fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
 - An unspecified address, such as ::/128
 - The loopback address, ::1/128
 - multicast addresses, ff00::/8
 - Link-local addresses, fe80::/10
- **Link-local**—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Network Discovery functions such as address resolution and neighbor discovery. In a bridge group, enabling IPv6 on the BVI automatically configures link-local addresses for each bridge group member interface. Each interface must have its own address because the link-local address is only available on a segment, and is tied to the interface MAC address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Management/Diagnostic Interface

The physical port labeled Management (or for Firepower Threat Defense Virtual, the Management0/0 virtual interface) actually has two separate interfaces associated with it.

- **Management virtual interface**—This IP address is used for system communication. This is the address the system uses for Smart Licensing and to retrieve database updates. You can open management sessions to it (Firepower Device Manager and CLI). You must configure a management address, which is defined on **System Settings > Management Interface**.
- **Diagnostic physical interface**—The physical Management port is actually named Diagnostic. You can use this interface to send syslog messages to an external syslog server. Configuring an IP address for the Diagnostic physical interface is optional. The only reason to configure the interface is if you want to use it for syslog. This interface appears, and is configurable, on the **Device > Interfaces** page. The Diagnostic physical interface only allows management traffic, and does not allow through traffic.

(Hardware devices.) The recommended way to configure Management/Diagnostic is to not wire the physical port to a network. Instead, configure the Management IP address only, and configure it to use the data interfaces as the gateway for obtaining updates from the Internet. Then, open the inside interfaces to HTTPS/SSH traffic (by default, HTTPS is enabled) and open Firepower Device Manager using the inside IP address (see [Configuring the Management Access List](#)).

For Firepower Threat Defense Virtual, the recommended configuration is to attach Management0/0 to the same network as the inside interface, and use the inside interface as the gateway. Do not configure a separate address for Diagnostic.

Recommendations for Configuring a Separate Management Network

(Hardware devices.) If you want to use a separate management network, wire the physical Management/Diagnostic interface to a switch or router.

For Firepower Threat Defense Virtual, attach Management0/0 to a separate network from any of the data interfaces. If you are still using the default IP addresses, you will need to change either the management IP address or the inside interface IP address, as they are on the same subnet.

Then, configure the following:

- Select **Device > System Settings > Management Interface** and configure IPv4 or IPv6 addresses (or both) on the attached network. If you want to, you can configure a DHCP server to provide IPv4 addresses to other endpoints on the network. If there is a router with a route to the internet on the management network, use that as the gateway. Otherwise, use the data interfaces as the gateway.
- Configure an address for the Diagnostic interface (on **Device > Interface**) only if you intend to send syslog messages through the interface to a syslog server. Otherwise, do not configure an address for Diagnostic, it is not needed. Any IP address you configure must be on the same subnet as the management IP address and cannot be in the DHCP server pool. For example, the default configuration uses 192.168.45.45 as the management address, and 192.168.45.46-192.168.45.254 as the DHCP pool, so you can configure Diagnostic using any address from 192.168.45.1 to 192.168.45.44.

Limitations for Management/Diagnostic Interface Configuration for a Separate Management Network

If you wire the physical Management interface, or for Firepower Threat Defense Virtual, you attach Management0/0 to a separate network, ensure that you follow these limitations:

- If you want a DHCP server on the management network, configure it on the Management interface (**Device > System Settings > Management Interface**). You cannot configure a DHCP server on the Diagnostic (physical) interface.
- If there is another DHCP server on the management network, disable it or the DHCP server running on Management. As a rule, a given subnet should have no more than one DHCP server.
- If you configure addresses for both Management and Diagnostic, ensure that they are on the same subnet.
- (Hardware devices only.) You can use the data interfaces as the management gateway even if you configure an IP address for Diagnostic. But Diagnostic will not use the data interfaces as a gateway. If you need a path from Diagnostic to other networks, another router on the management network needs to route the traffic originating from the Diagnostic IP address. If necessary, configure static routes for the Diagnostic interface (select **Device > Routing**).

Security Zones

Each interface can be assigned to a single security zone. You then apply your security policy based on zones. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. You can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside, for example.

For bridge groups, you add member interfaces to the zones, you cannot add the Bridge Virtual Interface (BVI).

You do not include the Diagnostic/Management interface in a zone. Zones apply to data interfaces only.

You can create security zones on the **Objects** page.

Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

About the MTU

The MTU specifies the maximum frame *payload* size that the Firepower Threat Defense device can transmit on a given Ethernet interface. The MTU value is the frame size *without* Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Path MTU Discovery

The Firepower Threat Defense device supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

MTU and Fragmentation

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.

**Note**

The Firepower Threat Defense device can receive frames larger than the configured MTU as long as there is room in memory.

MTU and Jumbo Frames

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all Firepower Threat Defense device interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames—A jumbo frame is an Ethernet packet larger than the standard maximum of 1522 bytes (including Layer 2 header and VLAN header), up to 9216 bytes. You can set the MTU up to 9198 bytes to accommodate jumbo frames. The maximum is 9000 for Firepower Threat Defense Virtual.



Note Increasing the MTU assigns more memory for jumbo frames, which might limit the maximum usage of other features, such as access rules. If you increase the MTU above the default 1500 on ASA 5500-X series devices or Firepower Threat Defense Virtual, you must reboot the system. You do not need to reboot Firepower 2100 series devices, where jumbo frame support is always enabled.

Guidelines and Limitations for Interfaces

The following topics cover some of the limitations for interfaces.

Limitations for Interface Configuration

When you use Firepower Device Manager to configure the device, there are several limitations to interface configuration. If you need any of the following features, you must use Firepower Management Center to configure the device.

- Routed firewall mode only is supported. You cannot configure transparent firewall mode interfaces.
- You cannot configure passive or ERSPAN interfaces.
- You cannot configure interfaces to be inline (in an inline set), or inline tap, for IPS-only processing. IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. In comparison, Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this firewall mode traffic according to your security policy.
- You cannot configure EtherChannel or redundant interfaces.
- You cannot configure PPPoE for IPv4. If the Internet interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, you must use Firepower Management Center to configure these settings.
- For the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X, you can install an optional network interface card (EPM). Cards are only discovered during bootstrap (that is, during installation, when switching between local/remote management, and during a major/minor release upgrade, but not patch or hot fix upgrades). For a card that includes SFP interfaces, Firepower Device Manager sets the speed and duplex

to auto; however, the SFP interfaces do not support the speed and duplex set to auto. For these interfaces, select the right speed (for example, 1000), or select **Default** for the speed and duplex. The Default setting tells Firepower Device Manager to simply not configure the options, and thus leave them at their default settings (any existing configuration is not cleared). Please refer to the EPM documentation to determine the maximum speed supported by the interface. You can also select **No Negotiate** for the speed setting if the interface accepts it, but select this option only if you are certain it is supported.



Note If you make a mistake and need to unconfigure **No Negotiate**, set the option to **Auto** and deploy. The deployment will fail. You can then set the option to **Default** and deploy again, and this should result in a successful deployment.

Maximum Number of VLAN Subinterfaces by Device Model

The device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface.

The following table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
ASA 5506-X	30
ASA 5506W-X	
ASA 5506H-X	
ASA 5506-X	30
ASA 5506W-X	
ASA 5506H-X	
ASA 5508-X	50
ASA 5512-X	100
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
Firepower 2100	1024
Firepower Threat Defense Virtual	50

Configuring Interfaces

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for it to pass traffic. If the interface is a member of a bridge group, this is sufficient. For non-bridge group members, you also need to give the interface an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs, which is useful when you connect to a trunk port on a switch.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, directly in the list of interfaces. The list shows the interface characteristics based on your configuration. Use the open/close arrow on a bridge group interface to view the member interfaces, which also appear by themselves in the list. For information on how these interfaces map to virtual interfaces and network adapters, see [How VMware Network Adapters and Interfaces Map to Firepower Threat Defense Physical Interfaces](#).

Use the port graphic to monitor the current state of the interfaces. Mouse over a port to see its IP addresses, and enabled and link statuses. The IP addresses can be statically assigned or obtained using DHCP.

Interface ports use the following color coding:

- Green—The interface is configured, enabled, and the link is up.
- Gray—The interface is not enabled.
- Orange/Red—The interface is configured and enabled, but the link is down. If the interface is wired, this is an error condition that needs correction. If the interface is not wired, this is the expected status.

The following topics explain how to configure interfaces.

Configure a Physical Interface

At minimum, you must enable a physical interface to use it. You would also typically name it and configure IP addressing. You would not configure IP addressing if you intend to create VLAN subinterfaces, or if you intend to add the interface to a bridge group.




Note You cannot configure IP addresses on bridge group member interfaces, although you can modify advanced settings as needed.

You can disable an interface to temporarily prevent transmission on the connected network. You do not need to remove the interface's configuration.

Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states.

Step 2 Click the edit icon () for the physical interface you want to edit.

Step 3 To enable the interface, click **Status > On**.

If you intend to configure subinterfaces for this physical interface, you are probably done. Click **Save** and continue with [Configure VLAN Subinterfaces and 802.1Q Trunking, on page 9](#). Otherwise, continue.

Note Even when configuring subinterfaces, it is valid to name the interface and supply IP addresses. This is not the typical setup, but if you know that is what you need, you can configure it.

Step 4 Configure the following:

- **Interface Name**—The name for the interface, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored. Unless you configure subinterfaces, the interface should have a name.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- (Optional.) **Description**—The description can be up to 200 characters on a single line, without carriage returns.

Step 5 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **Dynamic (DHCP)**—Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.
- **Static**—Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

Note For an existing interface, your ability to change the address is constrained if you have a DHCP server configured for the interface. The new IP address must be on the same subnet as the DHCP address pool, and it cannot be part of that pool. If you need to configure an address on a different subnet, first delete the DHCP server configuration. See [Configuring DHCP Server](#).

Step 6 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration**—Select this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FTD device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 2](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feec:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Suppress RA**—Whether to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 7 (Optional.) [Configure Advanced Interface Options, on page 15](#).

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 8 Click **OK**.

Configure VLAN Subinterfaces and 802.1Q Trunking

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.



Note You cannot configure IP addresses on bridge group member interfaces, although you can modify advanced settings as needed.

Before you begin


Preventing untagged packets on the physical interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, ensure that the physical interface does not pass traffic by not naming the interface. If you want to let the physical interface pass untagged packets, you can name the interface as usual.


Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states. Subinterfaces are grouped under their physical interface.

Step 2 Do one of the following:

- Select **Add Subinterface** from the gear drop-down list to create a new subinterface.
- Click the edit icon () for the subinterface you want to edit.

If you no longer need a subinterface, click the delete icon () for the subinterface to delete it.

Step 3 To enable the interface, click **Status > On**.

Step 4 Configure the parent interface, name, and description:

- **Parent Interface**—Choose the physical interface to which you want to add the subinterface. You cannot change the parent interface after you create the subinterface.
- **Name**—The name for the subinterface, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- (Optional.) **Description**—The description can be up to 200 characters on a single line, without carriage returns.

Step 5 Configure the general subinterface characteristics:

- **VLAN ID**—Enter the VLAN ID between 1 and 4094 that will be used to tag the packets on this subinterface.

- **Subinterface ID**—Enter the subinterface ID as an integer between 1 and 4294967295. The number of subinterfaces allowed depends on your platform. You cannot change the ID after you create the subinterface.

Step 6 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **Dynamic (DHCP)**—Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.
- **Static**—Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

Note For an existing interface, your ability to change the address is constrained if you have a DHCP server configured for the interface. The new IP address must be on the same subnet as the DHCP address pool, and it cannot be part of that pool. If you need to configure an address on a different subnet, first delete the DHCP server configuration. See [Configuring DHCP Server](#).

Step 7 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration**—Select this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FTD device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 2](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Suppress RA**—Whether to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 8 (Optional.) [Configure Advanced Interface Options, on page 15.](#)

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 9 Click **OK**.

Configure Bridge Groups

A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Thus, you can attach workstations or other endpoint devices directly to the interfaces included in the bridge group. You do not need to connect them through a separate physical switch, although you can also attach a switch to a bridge group member.

The group members do not have IP addresses. Instead, all member interfaces share the IP address of the Bridge Virtual Interface (BVI). If you enable IPv6 on the BVI, member interfaces are automatically assigned unique link-local addresses.

You typically configure a DHCP server on the bridge group interface (BVI), which provides IP addresses for any endpoints connected through member interfaces. However, you can configure static addresses on the endpoints connected to the member interfaces if you prefer. All endpoints within the bridge group must have IP addresses on the same subnet as the bridge group IP address.



Note For all ASA 5506-X models, on a new version 6.2+ system, or a reimaged 6.2+ system, the device comes pre-configured with bridge group BV11, named **inside**, which includes all data interfaces except for the **outside** interface. Thus, the device is pre-configured with one port used for linking to the Internet or other upstream network, and all other ports enabled and available for direct connections to endpoints. If you want to use an inside interface for a new subnet, you must first remove the needed interfaces from BV11.

Before you begin

Configure the interfaces that will be members of the bridge group. Specifically, each member interface must meet the following requirements:



- The interface must have a name.
- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP. If you need to remove the address from an interface that you are currently using, you might also need to remove other configurations for the interface, such as static routes, DHCP server, or NAT rules, that depend on the interface having an address.
- You must remove the interface from its security zone (if it is in a zone), and delete any NAT rules for the interface, before you can add it to a bridge group.

In addition, you enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.



Note You cannot configure bridge groups on Firepower 2100 series or Firepower Threat Defense Virtual devices.

Procedure

- Step 1** Click **Device**, then click the link in the **Interfaces** summary.
- The interface list shows the available interfaces, their names, addresses, and states. If there is already a bridge group, it is a folder. Click the open/close arrow to view the member interfaces. Member interfaces also appear separately in the list.
- Step 2** Do one of the following:
- Click the edit icon () for the BV11 bridge group.
 - Select **Add Bridge Group Interface** from the gear drop-down list to create a new group.
- Note** You can have a single bridge group. If you already have a bridge group defined, you should edit that group instead of trying to create a new one. If you need to create a new bridge group, you must first delete the existing bridge group.
- Click the delete icon () for the bridge group if you no longer need it. When you delete a bridge group, its members become standard routed interfaces, and any NAT rules or security zone membership are retained. You can edit the interfaces to give them IP addresses. If you want to add them to a new bridge group, first you need to remove the NAT rules and remove the interface from its security zone.
- Step 3** Configure the following:
- **Interface Name**—The name for the bridge group, up to 48 characters. Alphabetic characters must be lower case. For example, **inside** or **outside**. Without a name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- (Optional.) **Description**—The description can be up to 200 characters on a single line, without carriage returns.

Step 4 Edit the Bridge Group Members list.

You can add up to 64 interfaces or subinterfaces to a single bridge group.

- Click + to add an interface.
- Mouse over an interface you want to remove and click the **x** on the right side.

Step 5 Click the **IPv4 Address** tab and configure the IPv4 address.

Select one of the following options from the **Type** field:

- **Static**—Choose this option if you want to assign an address that should not change. Type in the bridge group's IP address and the subnet mask. All attached endpoints will be on this network. For models with a pre-configured bridge group, the default for the BVII “inside” network is 192.168.1.1/24 (i.e. 255.255.255.0). Ensure that the address is not already used on the network.

Note For an existing bridge group, your ability to change the address is constrained if you have a DHCP server configured for the group. The new IP address must be on the same subnet as the DHCP address pool, and it cannot be part of that pool. If you need to configure an address on a different subnet, first delete the DHCP server configuration. See [Configuring DHCP Server](#).

- **Dynamic (DHCP)**—Choose this option if the address should be obtained from the DHCP server on the network. This is not the typical option for bridge groups, but you can configure it if needed. Change the following options if necessary:
 - **Route Metric**—If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
 - **Obtain Default Route**—Whether to get the default route from the DHCP server. You would normally select this option, which is the default.

Step 6 (Optional.) Click the **IPv6 Address** tab and configure the IPv6 address.

- **State**—To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, select **Enabled**. The link local address is generated based on the interface MAC addresses (*Modified EUI-64* format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Static Address/Prefix**—If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see [IPv6 Addressing, on page 2](#).

If you want to use the address as link local only, select the **Link - Local** option. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Suppress RA**—Whether to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FTD device to supply the IPv6 prefix (for example, the outside interface).

Step 7 (Optional.) [Configure Advanced Interface Options, on page 15.](#)

You configure most advanced options on bridge group member interfaces, but some are available for the bridge group interface.

The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 8 Click **OK**.

What to do next

- Ensure that all member interfaces that you intend to use are enabled.
- Configure a DHCP server for the bridge group. See [Configuring DHCP Server](#).
- Add the member interfaces to the appropriate security zones. See [Configuring Security Zones](#).
- Ensure that policies, such as identity, NAT, and access, supply the required services for the bridge group and member interfaces.

Configure Advanced Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

Limitations

- For bridge groups, you configure most of these options on the member interfaces. Except for DAD attempts, these options are not available for the Bridge Virtual Interface (BVI).
- You cannot set MTU, duplex, or speed for the Management interface on a Firepower 2100 series device.

Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

The interface list shows the available interfaces, their names, addresses, and states.

Step 2 Click the edit icon () for the interface you want to edit.

Step 3 Click the **Advanced Options** tab.

Step 4 To make a data interface management only, select **Management Only**.

A management only interface does not allow through traffic, so there is very little value in setting a data interface as management only. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

Step 5 Change the **MTU** (maximum transmission unit) to the desired value.

The default MTU is 1500 bytes. You can specify a value from 64 - 9198 (or 9000, for Firepower Threat Defense Virtual). Set a high value if you typically see jumbo frames on your network.

Note If you increase MTU above 1500 on ASA 5500-X series devices or Firepower Threat Defense Virtual, you must reboot the device. Log into the CLI and use the **reboot** command. You do not need to reboot Firepower 2100 series devices, where jumbo frame support is always enabled.

Step 6 (Physical interface only.) Modify the speed and duplex settings.

The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. Before setting these options for interfaces on an EPM card, please read [Limitations for Interface Configuration, on page 5](#).

- **Duplex**—Choose **Auto**, **Half**, **Full**, or **Default**. Auto is the default when the interface supports it. For example, you cannot select Auto for the SFP interfaces on a Firepower 2100 series device.

Select **Default** to indicate that Firepower Device Manager should not attempt to configure the setting. Any existing configuration is left unchanged.

- **Speed**—Choose **Auto** to have the interface negotiate the speed (this is the default), or pick a specific speed: **10**, **100**, **1000**, **10000** Mbps. You can also select these special options:

- **No Negotiate**—For fiber interfaces, sets the speed to 1000 Mbps and does not negotiate link parameters. This is the default configured setting on these interfaces.
- **Default**—Indicates that Firepower Device Manager should not attempt to configure the setting. Any existing configuration is left unchanged.

The type of interface limits the options you can select. For example, the SFP+ interfaces on a Firepower 2100 series device support 1000 (1 Gbps) and 10000 (10 Gbps) only, and the SFP interfaces support 1000 (1 Gbps) only, whereas GigabitEthernet ports do not support 10000 (10 Gbps). SFP interfaces on other devices might require **No Negotiate**. Consult the hardware documentation for information on what the interfaces support.

Step 7 Modify the **IPv6 Configuration** settings.

- **Enable DHCP for IPv6 address configuration**—Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.
- **Enable DHCP for IPv6 non-address configuration**—Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.
- **DAD Attempts**—How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless autoconfiguration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

Step 8 Click **OK**.

Add Interfaces to Firepower Threat Defense Virtual

When you deploy a Firepower Threat Defense Virtual device, you assign interfaces to the virtual machine. Then, from within Firepower Device Manager, you configure those interfaces using the same methods you would use for a hardware device.

However, you cannot add more virtual interfaces to the virtual machine and then have Firepower Device Manager automatically recognize them. If you need more physical-interface equivalents for a Firepower Threat Defense Virtual device, you basically have to start over. You can either deploy a new virtual machine, or you can use the following procedure.



Caution

Adding interfaces to a virtual machine requires that you completely wipe out the Firepower Threat Defense Virtual configuration. The only part of the configuration that remains intact is the management address and gateway settings.

Before you begin

Do the following in Firepower Device Manager:

- Examine the Firepower Threat Defense Virtual configuration and make notes on settings that you will want to replicate in the new virtual machine.
- Select **Devices > Smart License > View Configuration** and disable all feature licenses.

Procedure

Step 1 Power off the Firepower Threat Defense Virtual device.

Step 2 Using the virtual machine software, add the interfaces to the Firepower Threat Defense Virtual device.

For VMware, virtual appliances use e1000 (1 Gbit/s) interfaces by default. You can also use vmxnet3 or ixgbe (10 Gbit/s) interfaces.

Step 3 Power on the Firepower Threat Defense Virtual device.

Step 4 Open the Firepower Threat Defense Virtual console, delete the local manager, then enable the local manager.

Deleting the local manager, then enabling it, resets the device configuration and gets the system to recognize the new interfaces. The management interface configuration does not get reset. The following SSH session shows the commands.

```
> show managers
Managed locally.
```

```
> configure manager delete
```

```
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
```

```
> show managers
No managers configured.
```

```
> configure manager local
>
```

Step 5 Open a browser session to Firepower Device Manager, complete the device setup wizard, and configure the device. See [Complete the Initial Configuration](#).

Monitoring Interfaces

You can view some basic information about interfaces in the following areas:

- **Monitoring > System.** The **Throughput** dashboard shows information on traffic flowing through the system. You can view information on all interfaces, or you can select a specific interface to examine.
- **Monitoring > Ingress Zones and Egress Zones.** These dashboards show statistics based on zones, which are composed of interfaces. You can drill into this information for more detail.
- **Device.** The Connection Diagram shows interface status. Mouse over a port to see the IP addresses for the interface, and the state of the interface and the link state. Use this information to help identify interfaces that are down when they should be up.

Monitoring Interfaces in the CLI

You can also log into the device CLI and use the following commands to get more detailed information about interface-related behavior and statistics.

- **show interface** displays interface statistics and configuration information. This command has many keywords you can use to get to the information you need. Use ? as a keyword to see the available options.
- **show ipv6 interface** displays IPv6 configuration information about the interfaces.

- **show bridge-group** displays information about Bridge Virtual Interfaces (BVI), including member information and IP addresses.
- **show conn** displays information about the connections currently established through the interfaces.
- **show traffic** displays statistics about traffic flowing through each interface.
- **show ipv6 traffic** displays statistics about IPv6 traffic flowing through the device.
- **show dhcpd** displays statistics and other information about DHCP usage on the interfaces, particularly about the DHCP servers configured on interfaces.

Examples for Interfaces

The use case chapter includes the following interface-related examples:

- [How to Configure the Device in Firepower Device Manager](#)
- [How to Add a Subnet](#)

