Interface Overview for Firepower Threat Defense

The Firepower Threat Defense device includes data interfaces that you can configure in different modes, as well as a management/diagnostic interface.

Management/Diagnostic Interface

he physical management interface is shared between the Diagnostic logical interface and the Management logical interface.

Management Interface

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firepower Management Center. It uses its own IP address and static routing. You can configure its settings at the CLI using the **configure network** command. If you change the IP address at the CLI after you add it to the Firepower Management Center, you can match the IP address in the Firepower Management Center in the **Devices** > **Device Management** > **Devices** > **Management** area.

Diagnostic Interface

The Diagnostic logical interface can be configured along with the rest of the data interfaces on the **Devices** > **Device Management** > **Interfaces** screen. Using the Diagnostic interface is optional (see the routed and transparent mode deployments for scenarios). The Diagnostic interface only allows management traffic, and does not allow through traffic. It does not support SSH; you can SSH to data interfaces or to the Management interface only. The Diagnostic interface is useful for SNMP or syslog monitoring.

Interface Mode and Types

You can deploy Firepower Threat Defense interfaces in two modes: Regular firewall mode and IPS-only mode. You can include both firewall and IPS-only interfaces on the same device.

Regular Firewall Mode

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 traffic according to your security policy.

The types of firewall interfaces you can configure depends on the firewall mode set for the device: routed or transparent mode. See Transparent or Routed Firewall Mode for Firepower Threat Defense for more information.

- Routed mode interfaces (routed firewall mode only)—Each interface that you want to route between is on a different subnet.
- Bridge group interfaces (routed and transparent firewall mode)—You can group together multiple interfaces on a network, and the Firepower Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. In routed mode, the Firepower Threat Defense device routes between BVIs and regular routed interfaces. In transparent mode, each bridge group is separate and cannot communicate with each other.

IPS-Only Mode

IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. You might want to implement IPS-only interfaces if you have a separate firewall protecting these interfaces and do not want the overhead of firewall functions.

Note The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes.

IPS-only interfaces can be deployed as the following types:

- Inline Set, with optional Tap mode—An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the FTD to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

  With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed. Instead, the FTD makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline. For example, you can set up the cabling between the FTD and the network as if the FTD were inline and analyze the kinds of intrusion events the FTD generates. Based on the results, you can modify your intrusion policy and add the drop rules that best protect your network without impacting its efficiency. When you are ready to deploy the FTD inline, you can disable tap mode and

begin dropping suspicious traffic without having to reconfigure the cabling between the FTD and the network.

Note Tap mode *significantly* impacts FTD performance, depending on the traffic.

Note Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode or the firewall-type interfaces.

- Passive or ERSPAN Passive—Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When you configure the FTD in a passive deployment, the FTD cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally. and no traffic received on these interfaces is retransmitted. Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches, and uses GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the FTD is in routed firewall mode.

Note Using SR-IOV interfaces as passive interfaces on NGFWv is not supported on some Intel network adapters (such as Intel X710 or 82599) using SR-IOV drivers due to a promiscuous mode restriction. In such cases, use a network adapter that supports this functionality. See Intel Ethernet Products for more information on Intel network adapters.

Security Zones and Interface Groups

Each interface can be assigned to a *security zone* and/or *interface group*. You then apply your security policy based on zones or groups. 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. Note that the interface or zone name itself does not provide any default behvior in regards to the security policy, we recommend using names that are self-describing to avoid mistakes in future configuration. A good name signifies a logical segment or traffic specification, for example:

- Names of internal interfaces—InsideV110, InsideV160, InsideV195
- Names of DMZ interfaces—DMZV11, DMZV12, DMZV-TEST
- Names of external interfaces—Outside-ASN78, Outside-ASN91

Some policies only support security zones, while other policies support zones and groups. For specifics, see Interface Objects: Interface Groups and Security Zones. You can create security zones and interface groups

on the **Objects** page. You can also add a zone when you are configuring the interface. You can only add interfaces to the correct zone type for your interface, either Passive, Inline, Routed, or Switched zone types.

Note Policies that apply to **any** zone (a global policy) apply to interfaces in zones as well as any interfaces that are not assigned to a zone.

The Diagnostic/Management interface does not belong to a zone or interface group.

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.

Default Settings for Interfaces

This section lists default settings for interfaces.

Default State of Interfaces

The default state of an interface depends on the type.

- Physical interfaces—Disabled. The exception is the interface that is enabled for initial setup.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- EtherChannel port-channel interfaces (ASA models)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Firepower models)—Disabled.

Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and in the FMC. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and FMC.

Default Speed and Duplex

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

By default, the speed and duplex for fiber (SFP) interfaces are set to the maximum speed, with auto-negotiation enabled.

Enable the Physical Interface and Configure Ethernet Settings

This section describes how to:

- Enable the physical interface. By default, physical interfaces are disabled (with the exception of the interface).
- Set a specific speed and duplex. By default, speed and duplex are set to Auto.

This procedure only covers a small subset of Interface settings. Refrain from setting other parameters at this point. For example, you cannot name an interface that you want to use as part of an EtherChannel or redundant interface.

Note For the Firepower 4100/9300, you configure basic interface settings in FXOS. See Configure a Physical Interface for more information.

Before you begin

If you changed the physical interfaces on the device after you added it to the FMC, you need to refresh the interface listing by clicking **Sync Interfaces from device** on the top left of **Interfaces**.

Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** ( ) for your Firepower Threat Defense device. The **Interfaces** page is selected by default.

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

Step 3 Enable the interface by checking the **Enabled** check box.

Step 4 (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.

- **Duplex**—Choose **Full**, **Half**, or **Auto**. Auto is the default for RJ-45 interfaces. You cannot select Auto for SFP interfaces.
- **Speed**—Choose **Auto** to have the interface negotiate the speed, link status, and flow control (Auto is only available for RJ-45 interfaces), or pick a specific speed: **10**, **100**, **1000**, **10000** Mbps. For SFP interfaces, setting the speed enables auto-negotiation of link status and flow control. For SFP interfaces, depending on your hardware, you can select **No Negotiate** to set the speed to 1000 and disable link negotiation.

Step 6 In the **Mode** drop-down list, choose one of the following:.

- **None**—Choose this setting for regular firewall interfaces and inline sets. The mode will automatically be changed to Routed, Switched, or Inline based on futher configuration.
- **Passive**—Choose this setting for passive IPS-only interfaces.
- **Erspan**—Choose this setting for ERSPAN passive IPS-only interfaces.

Step 7 Click **OK**.

Step 8 Click **Save**.

You can now click **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Step 9 Continue configuring interfaces.

- Regular Firewall Interfaces for Firepower Threat Defense
- Inline Sets and Passive Interfaces for Firepower Threat Defense

Sync Interface Changes with the Firepower Management Center

Interface configuration changes on the device can cause the FMC and the device to get out of sync. The FMC can detect interface changes by one of the following methods:

- Event sent from the device
- Sync when you deploy from the FMC

  If the FMC detects interface changes when it attempts to deploy, the deploy will fail. You must first accept the interface changes.
- Manual sync

Adding a new interface, or deleting an unused interface has minimal impact on the Firepower Threat Defense configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the Firepower Threat Defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the FMC.

This procedure describes how to manually sync device changes if required and how to acknowledge the detected changes. If device changes are temporary, you should not save the changes in the FMC; you should wait until the device is stable, and then re-sync.

Before you begin

- Model Support—FTD
- User Roles:

- Admin
- Access Admin
- Network Admin

Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** ( ) for your Firepower Threat Defense device. The **Interfaces** page is selected by default.

Step 2 If required, click **Sync Device** on the top left of **Interfaces**.

Step 3 After the changes are detected, see the following steps.

a) You will see a red banner on **Interfaces** indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.

b) Click **Save**.

You can now click **Deploy** and deploy the policy to assigned devices.