

Inline Sets and Passive Interfaces for Firepower Threat Defense

You can configure IPS-only passive interfaces, passive ERSPAN interfaces, and inline sets. 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.

- About IPS Interfaces, on page 1
- Guidelines for Inline Sets and Passive Interfaces, on page 2
- Configure a Passive Interface, on page 3
- Configure an Inline Set, on page 5

About IPS Interfaces

This section describes IPS interfaces.

IPS Interface Types

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.

Guidelines for Inline Sets and Passive Interfaces

Firewall Mode

- ERSPAN interfaces are only allowed when the device is in routed firewall mode.
- Firepower Threat Defense cannot load balance GRE traffic to multiple Rx rings. Flow-offload feature does not work for ERSPAN traffic. Hence, high rate of ERSPAN traffic can cause packet drop and impact the Firepower Threat Defense performance.

General Guidelines

- Inline sets and passive interfaces support physical interfaces only, and cannot use EtherChannels, redundant interfaces, VLANs, and so on.
- Inline sets and passive interfaces are supported in intra-chassis and inter-chassis clustering.
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firepower Threat Defense when using inline sets. If there are two neighbors on either side of the Firepower Threat Defense running BFD, then the Firepower Threat Defense will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.
- For inline sets and passive interfaces, the FTD supports up to two 802.1Q headers in a packet (also known as Q-in-Q support), with the exception of the Firepower 4100/9300, which only supports one 802.1Q header. **Note:** Firewall-type interfaces do not support Q-in-Q, and only support one 802.1Q header.

Unsupported Firewall Features on IPS Interfaces

- DHCP server
- DHCP relay
- DHCP client
- TCP Intercept
- Routing
- NAT
- VPN
- Application inspection
- QoS
- NetFlow
- VXLAN

Configure a Passive Interface

This section describes how to:

- Enable the interface. By default, interfaces are disabled.
- Set the interface mode to Passive or ERSPAN. For ERSPAN interfaces, you will set the ERSPAN parameters and the IP address.
- Change the MTU. By default, the MTU is set to 1500 bytes. For more information about the MTU, see About the MTU.
- Set a specific speed and duplex (if available). By default, speed and duplex are set to Auto.

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

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 In the **Mode** drop-down list, choose **Passive** or **Erspan**.

Step 4 Enable the interface by checking the **Enabled** check box.

Step 5 In the **Name** field, enter a name up to 48 characters in length.

Step 6 From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New**.

Step 7 (Optional) Add a description in the **Description** field.

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

Step 8 (Optional) On **General**, set the **MTU** between 64 and 9198 bytes; for the Firepower Threat Defense Virtual and Firepower Threat Defense on the FXOS chassis, the maximum is 9000 bytes.

The default is 1500 bytes.

Step 9 For ERSPAN interfaces, set the following parameters:

- **Flow Id**—Configure the ID used by the source and destination sessions to identify the ERSPAN traffic, between 1 and 1023. This ID must also be entered in the ERSPAN destination session configuration.
- **Source IP**—Configure the IP address used as the source of the ERSPAN traffic.

Step 10 For ERSPAN interfaces, set the IPv4 address and mask on **IPv4**.

Step 11 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.

The exact speed and duplex options depend on your hardware.

- **Duplex**—Choose **Full**, **Half**, or **Auto**. Auto is the default.
- **Speed**—Choose **10**, **100**, **1000**, or **Auto**. Auto is the default.

Step 12 Click **OK**.

Step 13 Click **Save**.

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

Configure an Inline Set

This section enables and names two physical interfaces that you can add to an inline set.

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

Before you begin

- We recommend that you set STP PortFast for STP-enabled switches that connect to the FTD inline pair 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 In the **Mode** drop-down list, choose **None**.

After you add this interface to an inline set, this field will show Inline for the mode.

Step 4 Enable the interface by checking the **Enabled** check box.

Step 5 In the **Name** field, enter a name up to 48 characters in length.

Do not set the security zone yet; you must set it after you create the inline set later in this procedure.

Step 6 (Optional) Add a description in the **Description** field.

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

Step 7 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.

The exact speed and duplex options depend on your hardware.

- **Duplex**—Choose **Full**, **Half**, or **Auto**. Auto is the default.
- **Speed**—Choose **10**, **100**, **1000**, or **Auto**. Auto is the default.

Step 8 Click **OK**.

Do not set any other settings for this interface.

Step 9 Click **Edit** ( ) for the second interface you want to add to the inline set.

Step 10 Configure the settings as for the first interface.

Step 11 Click **Inline Sets**.

Step 12 Click **Add Inline Set**.

The **Add Inline Set** dialog box appears with **General** selected.

Step 13 In the **Name** field, enter a name for the set.

Step 14 (Optional) Change the **MTU** to enable jumbo frames.

For inline sets, the MTU setting is not used. However, the jumbo frame setting *is* relevant to inline sets; jumbo frames enable the inline interfaces to receive packets up to 9000 bytes. To enable jumbo frames, you must set the MTU of *any* interface on the device above 1500 bytes.

Step 15 (Optional) To specify that traffic is allowed to bypass detection and continue through the device in the case of a sensor failure, check the **Failsafe** check box.

Managed devices monitor internal traffic buffers and bypass detection if those buffers are full.

Step 16 In the **Available Interfaces Pairs** area, click a pair and then click **Add** to move it to the **Selected Interface Pair** area.

All possible pairings between named and enabled interfaces with the mode set to None show in this area.

Step 17 (Optional) Click **Advanced** to set the following optional parameters:

- **Tap Mode**—Set to inline tap mode.

  Note that you cannot enable this option and strict TCP enforcement on the same inline set.

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

- **Propagate Link State**—Configure link state propagation.

  Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the device senses the change and updates the link state of the other interface to match it. Note that devices require up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

  Note This feature is not supported on the Firepower 4100/9300 chassis.

- **Strict TCP Enforcement**—To maximize TCP security, you can enable strict enforcement, which blocks connections where the three-way handshake was not completed.

  Strict enforcement also blocks:

  - Non-SYN TCP packets for connections where the three-way handshake was not completed
  - Non-SYN/RST packets from the initiator on a TCP connection before the responder sends the SYN-ACK
  - Non-SYN-ACK/RST packets from the responder on a TCP connection after the SYN but before the session is established
  - SYN packets on an established TCP connection from either the initiator or the responder

Step 18 Click **Interfaces**.

Step 19 Click **Edit** () for one of the member interfaces.

Step 20 From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New**.

You can only set the zone after you add the interface to the inline set; adding it to an inline set configures the mode to Inline and lets you choose inline-type security zones.

Step 21 Click **OK**.

Step 22 Set the security zone for the second interface.

Step 23 Click **Save**.

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