

Inline Sets and Passive Interfaces

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

- IPS interfaces, on page 1
- Requirements and prerequisites for inline sets, on page 5
- Guidelines for configuring inline sets and passive interfaces, on page 7
- Configure a passive interface, on page 9
- Configure Inline Sets, on page 10

IPS interfaces

Intrusion Prevention System (IPS) interfaces include passive interfaces, passive Enhanced Remote Switch Port Analyzer (ERSPAN) interfaces, and inline sets. Interfaces in IPS-only mode bypass many firewall checks and support only IPS security policy (Snort). Implement IPS-only interfaces if you have a separate firewall protecting these interfaces and want to avoid firewall function overhead.

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.

Inline sets

An inline set acts like a bump on the wire and binds one or more interface pairs together to slot into an existing network. This function allows the Firewall Threat Defense to be installed in any network environment without requiring configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally and retransmit all traffic out of the other interface in the inline pair unless traffic is explicitly dropped. When you have multiple inline pairs in an inline set, traffic can only pass between the interfaces in the pair; it can't pass between interfaces in different pairs.

Tap mode functionality

With tap mode, the Firewall Threat Defense is deployed inline, but the network traffic flow is undisturbed. Instead, the Firewall Threat Defense 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 Firewall Threat Defense that are deployed inline:

- You can set up the cabling between the Firewall Threat Defense and the network as if the Firewall Threat Defense were inline and analyze the kinds of intrusion events the Firewall Threat Defense 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 Firewall Threat Defense inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the Firewall Threat Defense and the network.



Note Tap mode *significantly* impacts Firewall Threat Defense 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.

Multiple inline pairs and asynchronous routing

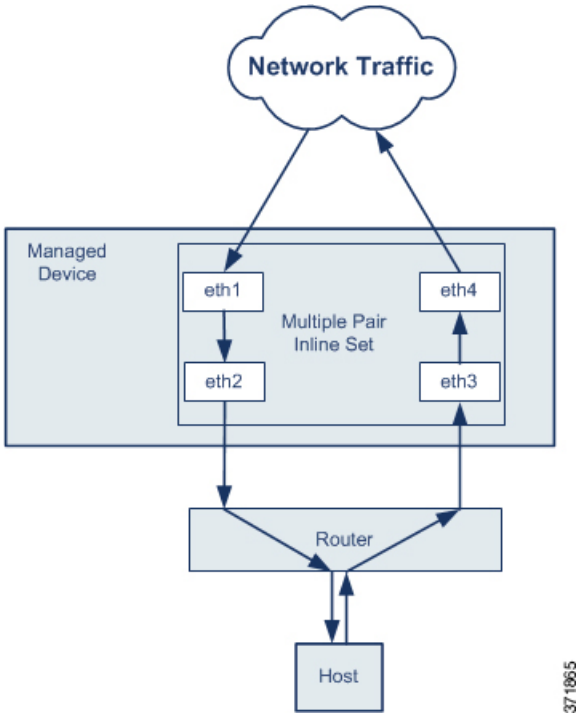
Asynchronous routing is a network configuration that routes traffic between a host on your network and external hosts through different inline pairs, depending on whether the traffic is inbound or outbound. It requires multiple inline pairs in an inline set to correctly analyze network traffic.

If you deploy asynchronous routing, but you include only one inline pair in an inline set, the device might not correctly analyze your network traffic because it might see only half of the traffic.

Multiple inline pairs configuration

Adding multiple inline pairs to the same inline set lets the system identify the inbound and outbound traffic as part of the same traffic flow. For passive interfaces only, you can also achieve this by including the interface pairs in the same security zone.

Figure 1: Asynchronous routing



Note If you assign multiple inline pairs to a single inline set, but you experience issues with duplicate traffic, you might need to reassign your inline pairs to separate inline sets or modify your security zones.

If fragments of a packet are received on different interface pairs, they are not reassembled and get dropped. Make sure all the fragments of the packet are received and sent on the same interface pair.

Passive interfaces

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 allows the system to view network traffic without participating in the flow of data.

Passive interface functionality

The SPAN or mirror port allows for traffic to be copied from other ports on the switch. When you configure the Firewall Threat Defense in a passive deployment, the Firewall Threat Defense cannot take certain actions such as blocking or shaping traffic.

Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches and use GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the Firewall Threat Defense 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.

Hardware Bypass for inline sets

Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. It maintains network connectivity when software or hardware failures occur and is available for certain interface modules on supported models.

Supported interface modules

For information about which interface modules support this feature, see Requirements and prerequisites for inline sets, on page 5.

Hardware Bypass triggers

Hardware Bypass can be triggered in these scenarios.

- Firewall Threat Defense crash
- Firewall Threat Defense reboot
- Security Module reboot
- Chassis crash
- Chassis reboot
- Manual trigger
- Chassis power loss
- Security Module power loss

Note Hardware bypass is intended for unplanned/unexpected failure scenarios, and is not automatically triggered during planned software upgrades. Hardware bypass activates only at the end of a planned upgrade process, when the Firewall Threat Defense application reboots.

Hardware bypass switchover

When you switch from normal operation to hardware bypass, or back to normal operation, you may experience several seconds of interrupted traffic. During this time, connections may drop.

Connection interruption factors

Several factors can affect the length of the traffic interruption during hardware bypass switchover.

- Copper port auto-negotiation
- Behavior of the optical link partner such as how it handles link faults and de-bounce timing
- Spanning tree protocol convergence
- Dynamic routing protocol convergence

You may also experience dropped connections due to application identification errors when analyzing connections midstream after the returning to normal operations.

Snort Fail Open vs. Hardware Bypass

Snort Fail Open and Hardware Bypass allow traffic to flow during system failures.

Functionality differences

You can configure the Snort Fail Open option for inline sets other than those in tap mode. This option either drops traffic or allows traffic to pass without inspection when the Snort process is busy or down. Snort Fail Open is supported on all inline sets except those in tap mode, not just on interfaces that support Hardware Bypass.

The Hardware Bypass functionality allows traffic to flow during a hardware failure, including a complete power outage, and certain limited software failures. A software failure that triggers Snort Fail Open does not trigger a Hardware Bypass.

Hardware Bypass status

When the system has power, the Bypass LED indicates the Hardware Bypass status. See the Firepower chassis hardware installation guide for LED descriptions.

Requirements and prerequisites for inline sets

This reference provides the requirements and prerequisites that must be met before configuring inline sets, including user role permissions and hardware bypass support information.

User roles

- Administrator
- Access Admin
- Network Admin

Hardware Bypass Support

The Firewall Threat Defense supports Hardware Bypass for interface pairs on specific network modules on the following models:

- Firepower 2130 and 2140
- Secure Firewall 3100
- Firepower 4100

- Secure Firewall 4200
- Firepower 9300
- Secure Firewall 6100

Note The ISA 3000 has a separate implementation for Hardware Bypass, which you can enable using FlexConfig only (see FlexConfig policies). Do not use this chapter to configure ISA 3000 Hardware Bypass.

Note You can use Hardware Bypass interfaces as regular interfaces without the Hardware Bypass feature enabled.

The supported Hardware Bypass network modules for these models include:

- Firepower 2130 and 2140:
  - Firepower 6-port 1G SX FTW Network Module single-wide (FPR2K-NM-6X1SX-F)
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR2K-NM-6X10SR-F)
  - Firepower 6-port 10G LR FTW Network Module single-wide (FPR2K-NM-6X10LR-F)
- Secure Firewall 3100:
  - 6-port 1G SFP Fail-to-Wire Network Module, SX (multimode) (FPR3K-XNM-6X1SXF)
  - 6-port 10G SFP Fail-to-Wire Network Module, SR (multimode) (FPR3K-XNM-6X10SRF)
  - 6-port 10G SFP Fail-to-Wire Network Module, LR (single mode) (FPR3K-XNM-6X10LRF)
  - 6-port 25G SFP Fail-to-Wire Network Module, SR (multimode) (FPR3K-XNM-X25SRF)
  - 6-port 25G Fail-to-Wire Network Module, LR (single mode) (FPR3K-XNM-6X25LRF)
  - 8-port 1G Copper Fail-to-Wire Network Module, RJ45 (copper) (FPR3K-XNM-8X1GF)
- Secure Firewall 4200:
  - 6-port 1G SFP Fail-to-Wire Network Module, SX (multimode) (FPR4K-XNM-6X1SXF)
  - 6-port 10G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-6X10SRF)
  - 6-port 10G SFP Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X10LRF)
  - 6-port 25G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-X25SRF)
  - 6-port 25G Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X25LRF)
  - 8-port 1G Copper Fail-to-Wire Network Module, RJ45 (copper) (FPR4K-XNM-8X1GF)
- Firepower 4100:
  - Firepower 6-port 1G SX FTW Network Module single-wide (FPR4K-NM-6X1SX-F)
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR4K-NM-6X10SR-F)

- Firepower 6-port 10G LR FTW Network Module single-wide (FPR4K-NM-6X10LR-F)
- Firepower 2-port 40G SR FTW Network Module single-wide (FPR4K-NM-2X40G-F)
- Firepower 8-port 1G Copper FTW Network Module single-wide (FPR-NM-8X1G-F)

- Secure Firewall 6100:
  - 6-port 1G SFP Fail-to-Wire Network Module, SX (multimode) (FPR4K-XNM-6X1SXF)
  - 6-port 10G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-6X10SRF)
  - 6-port 10G SFP Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X10LRF)
  - 6-port 25G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-X25SRF)
  - 6-port 25G Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X25LRF)
  - 8-port 1G Copper Fail-to-Wire Network Module, RJ45 (copper) (FPR4K-XNM-8X1GF)

- Firepower 9300:
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR9K-NM-6X10SR-F)
  - Firepower 6-port 10G LR FTW Network Module single-wide (FPR9K-NM-6X10LR-F)
  - Firepower 2-port 40G SR FTW Network Module single-wide (FPR9K-NM-2X40G-F)

Hardware Bypass can only use the following port pairs:

- 1 & 2
- 3 & 4
- 5 & 6
- 7 & 8

Guidelines for configuring inline sets and passive interfaces

Firewall mode restrictions

Use ERSPAN interfaces only when the device is in routed firewall mode.

Clustering restrictions

Consider clustering limitations when configuring inline sets and passive interfaces.

- Link State Propagation for an inline set is not supported with clustering.

Multi-Instance mode restrictions

Use unshared physical interfaces or EtherChannels when configuring multi-instance mode.

- Multi-instance shared interfaces are not supported. You must use an unshared interface.

- Multi-instance chassis-defined subinterfaces are not supported. You must use a physical interface or EtherChannel.

General configuration guidelines

Consider these interface and traffic inspection requirements when configuring inline sets and passive interfaces.

- Inline sets and passive interfaces support only physical interfaces and EtherChannels. You cannot use VLANs or other virtual interfaces, including multi-instance chassis-defined subinterfaces.
- Because IPS interfaces do not support regular firewall protections, traffic must pass through the same Firewall Threat Defense to ensure all traffic is inspected according to the IPS security policy (Snort).
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firewall Threat Defense when using inline sets. If there are two neighbors on either side of the Firewall Threat Defense running BFD, then the Firewall 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 Firewall Threat Defense 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.
- Firewall Threat Defense does not support frames with Ethertype 0x8988. If a source in the Application Centric Infrastructure (ACI) fabric has Precision Time Protocol (PTP) enabled, ACI inserts Ethertype 0x8988 into data-plane frames before mirroring. Firewall Threat Defense drops frames with Ethertype 0x8988 and does not inspect them.

Hardware Bypass Guidelines

Consider Hardware Bypass limitations and clustering requirements when configuring inline sets.

- Hardware Bypass ports are supported only for inline sets.
- Hardware Bypass ports cannot be part of an EtherChannel.
- Hardware Bypass is not supported in high availability mode.
- Hardware Bypass ports are supported with intra-chassis clustering on the Firepower 9300. Ports are placed in Hardware Bypass mode when the last unit in the chassis fails. Inter-chassis clustering is not supported, because inter-chassis clustering only supports Spanned EtherChannels; Hardware Bypass ports cannot be part of an EtherChannel.
- If all modules in an intra-chassis cluster on the Firepower 9300 fail, then Hardware Bypass is triggered on the final unit, and traffic continues to pass. When units come back up, Hardware Bypass returns to standby mode. If rules matching application traffic are used, connections might be dropped and require reestablishment. Connections are dropped because state information is not retained on the cluster unit, and the unit cannot identify the traffic as belonging to an allowed application. To prevent a traffic drop, use a port-based rule instead of an application-based rule, if appropriate for your deployment.
- You can use Hardware Bypass interfaces as regular interfaces without the Hardware Bypass feature enabled.

Unsupported firewall features on IPS interfaces

These firewall features are not supported on IPS interfaces.

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

Configure a passive interface

Configure a passive or ERSPAN interface to enable network monitoring and traffic analysis capabilities on your security device.

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 MTU.
- Set a specific speed and duplex (if available). By default, speed and duplex are set to Auto.



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

Before you begin

- If you are using EtherChannels, add them according to Configure an EtherChannel.

Follow these steps to configure a passive interface:

Procedure

Step 1 On the Cloud-Delivered Firewall Management Center, choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall 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.

Set these values:

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

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

c. 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) On **General**, set the **MTU** between 64 and 9198 bytes; for the Secure Firewall Threat Defense Virtual and Secure Firewall Threat Defense on the FXOS chassis, the maximum is 9000 bytes.

The default is 1500 bytes.

Step 6 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.
- **IPv4**—Set the IPv4 address and mask

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**.

Step 9 Click **Save**.

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

Configure Inline Sets

Enable traffic inspection by configuring multiple inline sets using physical interfaces or EtherChannels, including optional Hardware Bypass.

Inline sets allow you to designate pairs of interfaces or EtherChannels for traffic inspection, with optional Hardware Bypass. You can configure multiple inline pairs per set.

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

Before you begin

- If you are using EtherChannels, add them according to Configure an EtherChannel .
- We recommend that you set STP PortFast for STP-enabled switches that connect to the Firewall Threat Defense inline pair interfaces. This setting is especially useful for Hardware Bypass configurations and can reduce bypass times.

Procedure

Step 1 On the Cloud-Delivered Firewall Management Center, choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 For each interface in the inline pair, name the interface and enable it. Also configure necessary hardware settings, ensuring they match between interfaces in the inline pair. You can configure multiple pairs of interfaces.

a) Click **Edit** (✎) for the interface you want to edit.
b) In the **Name** field, enter a name up to 48 characters in length.
c) Enable the interface by checking the **Enabled** check box.
d) (Optional) Add a description in the **Description** field.

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

e) Leave the **Mode** as **None** .

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

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

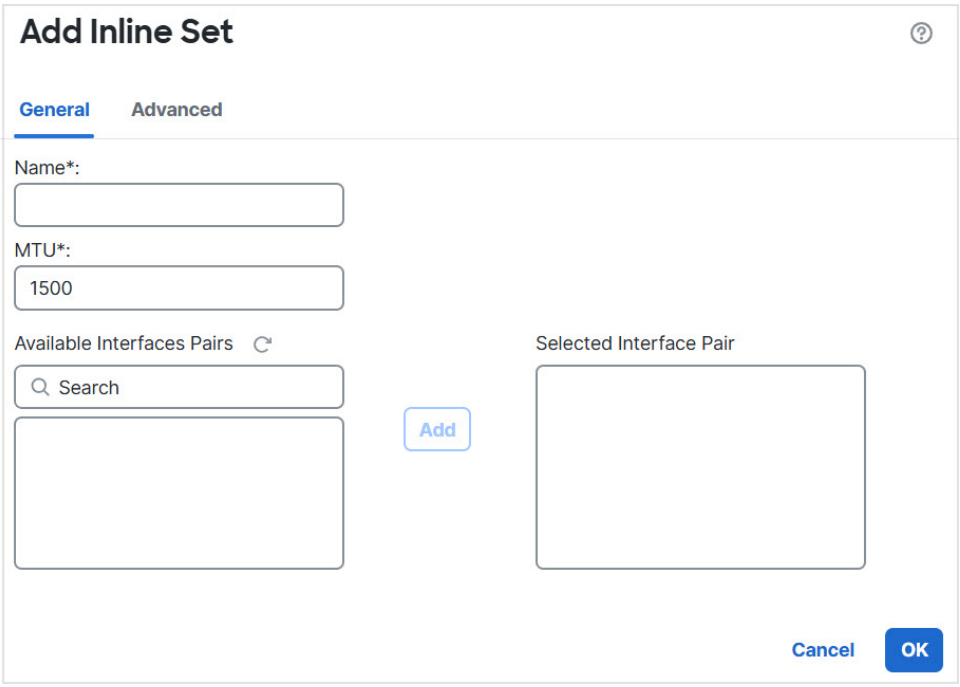
h) Click **OK** .

Do not set any other settings for this interface.

Step 3 Click **Inline Sets**.

Step 4 Click **Add Inline Set**.

Figure 2: Add Inline Set



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

Step 5 In the **Name** field, enter a name for the set.

Step 6 (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 7 Configure Hardware Bypass.

a) For the **Bypass** mode, choose one of the following options:

- **Disabled** —Set Hardware Bypass to disabled for interfaces where Hardware Bypass is supported, or use interfaces where Hardware Bypass is not supported.
- **Standby** —Set Hardware Bypass to the standby state on supported interfaces. Only pairs of Hardware Bypass interfaces are shown. In the standby state, the interfaces remain in normal operation until there is a trigger event.
- **Bypass-Force** —Manually forces the interface pair to go into a bypass state. **Inline Sets** shows **Yes** for any interface pairs that are in Bypass-Force mode.

b) 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 8 (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 Perform Tap mode changes during a maintenance window. Changing the mode while the device is passing traffic can cause traffic disruption.

Note Tap mode significantly impacts the Firewall Threat Defense 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 Do not enable **Propagate Link State** when using clustering.

- **Snort Fail Open** —Enable or disable either or both of the **Busy** and **Down** options if you want new and existing traffic to pass without inspection (enabled) or drop (disabled) when the Snort process is busy or down.

  By default, traffic passes without inspection when the Snort process is down, and drops when it is busy.

  When the Snort process is:

  - Busy—It cannot process traffic fast enough because traffic buffers are full, indicating that there is more traffic than the device can handle, or because of other software resource issues.
  - Down—It is restarting because you deployed a configuration that requires it to restart. See Configurations that restart the snort process when deployed or activated .

  When the Snort process is down and comes back up, it inspects *new* connections. To prevent false positives and false negatives, it does not inspect existing connections on inline, routed, or transparent interfaces because initial session information might have been lost while it was down.

Note When Snort fails open, features that rely on the Snort process do not function. These include application control and deep inspection. The system performs only basic access control using simple, easily determined transport and network layer characteristics.

Note The **Strict TCP Enforcement** option is not supported.

Step 9 Set the security zone for each interface.

a) Click **Interfaces** .

b) Click **Edit** ( ) for the member interface.

c) 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.

d) Click **OK** .

Click **Save**.

What to do next

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