

IPS Device Deployments and Configuration

The following topics describe how to configure your device in an IPS deployment:

- Introduction to IPS Device Deployment and Configuration, on page 1
- License Requirements for IPS Device Deployment, on page 1
- Requirements and Prerequisites for IPS Device Deployment, on page 1
- Passive IPS Deployments, on page 2
- Inline IPS Deployments, on page 4

Introduction to IPS Device Deployment and Configuration

You can configure your device in either a passive or inline IPS deployment. In a passive deployment, you deploy the system out of band from the flow of network traffic. In an inline deployment, you configure the system transparently on a network segment by binding two ports together.

License Requirements for IPS Device Deployment

FTD License

Threat

Classic License

Protection

Requirements and Prerequisites for IPS Device Deployment

Model Support

Any.

Supported Domains

Leaf.

User Roles

- Admin
- Network Admin

Passive IPS Deployments

In a passive IPS deployment, the Firepower System monitors traffic flowing across a network using a switch SPAN (or mirror) port. The SPAN port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system 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. Passive interfaces support both local SPAN and remote SPAN (RSPAN) traffic.

Note Outbound traffic includes flow control packets. Because of this, passive interfaces on your appliances may show outbound traffic and, depending on your configuration, generate events; this is expected behavior.

Passive Interfaces on the Firepower System

You can configure one or more physical ports on a managed device as passive interfaces.

When you enable a passive interface to monitor traffic, you designate mode and MDI/MDIX settings, which are available only for copper interfaces. Interfaces on 8000 Series appliances do not support half-duplex options.

When you disable a passive interface, users can no longer access it for security purposes.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Configuring Passive Interfaces

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to configure the passive interface.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Edit** ( ) next to the interface you want to configure as a passive interface.

Step 4 Click **Passive**.

Step 5 If you want to associate the passive interface with a security zone, do one of the following:

- Choose an existing security zone from the **Security Zone** drop-down list.
- Choose **New** to add a new security zone; see Creating Security Zone Objects.

Step 6 Check the **Enabled** check box.

If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.

Step 7 7000 & 8000 Series only: From the **Mode** drop-down list, designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to automatically negotiate speed and duplex settings.

Mode settings are available only for copper interfaces.

Interfaces on 8000 Series appliances do not support half-duplex options.

Step 8 7000 & 8000 Series only: From the **MDI/MDIX** drop-down list, designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

MDI/MDIX settings are available only for copper interfaces.

By default, MDI/MDIX is set to **Auto-MDIX**, which automatically handles switching between MDI and MDIX to attain link.

Step 9 Enter a maximum transmission unit (MTU) in the **MTU** field.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Step 10 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Inline IPS Deployments

In an inline IPS deployment, you configure the Firepower System transparently on a network segment by binding two ports together. This allows the system 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.

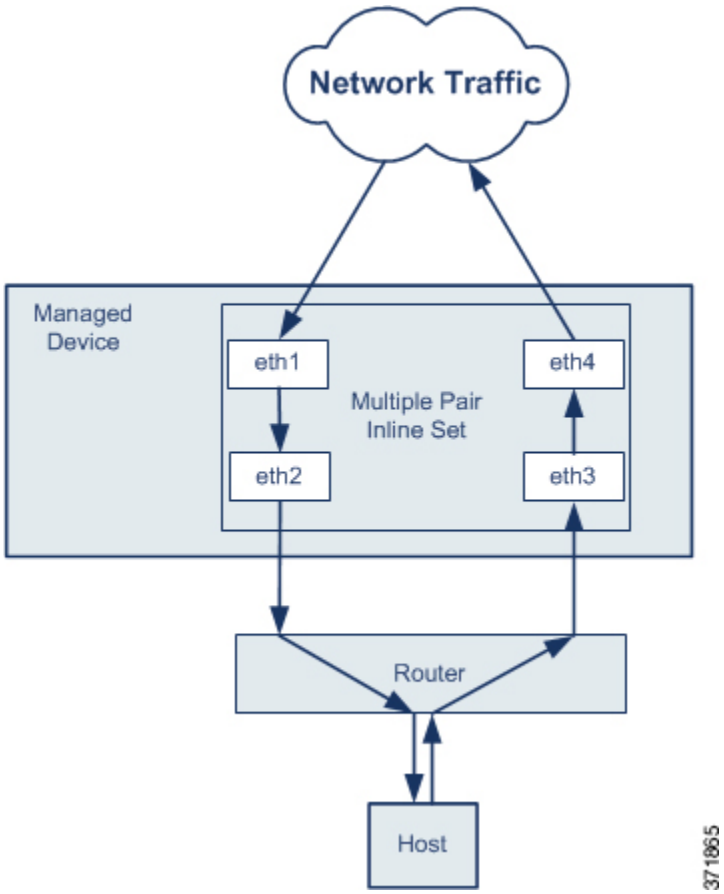


Note For the system to affect traffic, you must deploy relevant configurations to managed devices using routed, switched, or transparent interfaces, or inline interface pairs.

You can configure the interfaces on your managed device to route traffic between a host on your network and external hosts through different inline interface pairs, depending on whether the device traffic is inbound or outbound. This is an *asynchronous routing* configuration. If you deploy asynchronous routing but you include only one interface pair in an inline set, the device might not correctly analyze your network traffic because it might see only half of the traffic.

Adding multiple inline interface pairs to the same inline interface set allows the system to 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.

When the system generates a connection event from traffic passing through an asynchronous routing configuration, the event may identify an ingress and egress interface from the same inline interface pair. The configuration in the following diagram, for example, would generate a connection event identifying **eth3** as the ingress interface and **eth2** as the egress interface. This is expected behavior in this configuration.



Note If you assign multiple interface pairs to a single inline interface set but you experience issues with duplicate traffic, reconfigure to help the system uniquely identify packets. For example, you could reassign your interface pairs to separate inline sets or modify your security zones.

For devices with inline sets, a software bridge is automatically set up to transport packets after the device restarts. If the device is restarting, there is no software bridge running anywhere. If you enable bypass mode on the inline set, it goes into hardware bypass while the device is restarting. In that case, you may lose a few seconds of packets as the system goes down and comes back up, due to renegotiation of link with the device. However, the system will pass traffic while Snort is restarting.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Inline Interfaces on the Firepower System

You can configure one or more physical ports on a managed device as inline interfaces. You must assign a pair of inline interfaces to an inline set before they can handle traffic in an inline deployment.

Note:

- The system warns you if you set the interfaces in an inline pair to different speeds or if the interfaces negotiate to different speeds.
- If you configure an interface as an inline interface, the adjacent port on its NetMod automatically becomes an inline interface as well to complete the pair.
- To configure inline interfaces on an NGIPSv device, you must create the inline pair using adjacent interfaces.

Configuring Inline Interfaces

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to configure the interface.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Edit** ( ) next to the interface you want to configure.

Step 4 Click **Inline**.

Step 5 If you want to associate the inline interface with a security zone, do one of the following:

- Choose an existing security zone from the **Security Zone** drop-down list.
- Choose **New** to add a new security zone; see Creating Security Zone Objects.

Step 6 Choose an existing inline set from the **Inline Set** drop-down list, or choose **New** to add a new inline set.

Note If you add a new inline set, you must configure it after you set up the inline interface; see Adding Inline Sets, on page 8.

Step 7 Check the **Enabled** check box.

If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.

Step 8 7000 & 8000 Series only: From the **Mode** drop-down list, designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to automatically negotiate speed and duplex settings.

Mode settings are available only for copper interfaces.

Interfaces on 8000 Series appliances do not support half-duplex options.

Step 9 7000 & 8000 Series only: From the **MDI/MDIX** drop-down list, designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

MDI/MDIX settings are available only for copper interfaces.

By default, MDI/MDIX is set to **Auto-MDIX**, which automatically handles switching between MDI and MDIX to attain link.

Step 10 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Inline Sets

Before you can use inline interfaces in an inline deployment, you must configure inline sets and assign inline interface pairs to them. An inline set is a grouping of one or more inline interface pairs on a device; an inline interface pair can belong to only one inline set at a time.

The **Inline Sets** tab of the Device Management page displays a list of all inline sets you have configured on a device.

You can add inline sets from the **Inline Sets** tab of the Device Management page or you can add inline sets as you configure inline interfaces.

You can assign **only** inline interface pairs to an inline set. If you want to create an inline set before you configure the inline interfaces on your managed devices, you can create an empty inline set and add interfaces to it later. You can use alphanumeric characters and spaces when you type a name for an inline set.

Note Create inline sets before you add security zones for the interfaces in the inline set; otherwise security zones are removed and you must add them again.

Name

The name of the inline set.

Interfaces

A list of all inline interface pairs assigned to the inline set. A pair is not available when you disable either interface in the pair from the Interfaces tab.

MTU

The maximum transmission unit for the inline set. The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Failsafe

Allows traffic to bypass detection and continue through the device. Managed devices monitor internal traffic buffers and bypass detection if those buffers are full.

Bypass Mode

Firepower 7000 or 8000 Series only: The configured bypass mode of the inline set. This setting determines how the relays in the inline interfaces respond when an interface fails. The bypass mode allows traffic to continue to pass through the interfaces. The non-bypass mode blocks traffic.

Caution In bypass mode, you may lose a few packets when you reboot the appliance. You cannot configure bypass mode for inline sets on 7000 or 8000 Series devices in a high-availability pair, for non-bypass NetMods on 8000 Series devices, or for SFP modules on Firepower 7115 or 7125 devices.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Viewing Inline Sets

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to view the inline sets.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Inline Sets**.

Adding Inline Sets

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to add the inline set.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Inline Sets**.

Step 4 Click **Add Inline Set**.

Step 5 Enter a **Name**.

Step 6 Next to **Interfaces**, choose one or more inline interface pairs, then click **Add Selected**. To add all interface pairs to the inline set, click **Add All**.

Tip To remove inline interfaces from the inline set, choose one or more inline interface pairs and click **Remove Selected**. To remove all interface pairs from the inline set, click **Remove All**. Disabling either interface in a pair from **Interfaces** also removes the pair.

Step 7 Enter a maximum transmission unit (MTU) in the **MTU** field.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Step 8 If you want to specify that traffic is allowed to bypass detection and continue through the device, choose **Failsafe**.

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

Step 9 (7000/8000 series only) Specify the bypass mode.

- Click **Bypass** to allow traffic to continue to pass through the interfaces.
- Click **Non-Bypass** to block traffic.

Note You cannot configure bypass mode for inline sets on 7000 or 8000 Series devices in high-availability pairs, inline sets on an NGIPSv device, for non-bypass NetMods on 8000 Series devices, or for SFP modules on Firepower 7115 or 7125 devices.

Step 10 Optionally, configure advanced settings; see Advanced Inline Set Options, on page 9.

Step 11 Click **OK**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Advanced Inline Set Options

There are a number of advanced options you may consider as you configure inline sets.

Tap Mode

Tap mode is available on 7000 and 8000 Series devices when you create an inline or inline with fail-open interface set.

With tap mode, the device is deployed inline, but instead of the packet flow passing through the device, a copy of each packet is sent to the device and the network traffic flow is undisturbed. Because you are working with copies of packets rather than the packets themselves, rules that you set to drop and rules that use the replace keyword do not affect the packet stream. However, 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 devices that are deployed inline. For example, you can set up the cabling between the device and the network as if the device were inline and analyze the kinds of intrusion events the device 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 device inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the device and the network.

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

Propagate Link State



Note Link state propagation is not supported on virtual devices. Only 7000 and 8000 Series devices support link state propagation.

Link state propagation is a feature for inline sets configured in bypass mode and non-bypass mode so both pairs of an inline set track state. Link state propagation is available for both copper and fiber configurable bypass interfaces.

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 appliance senses the change and updates the link state of the other interface to match it. Note that appliances 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.

You cannot disable link state propagation for inline sets configured on 7000 and 8000 Series devices in high-availability pairs.

Transparent Inline Mode

Transparent Inline Mode option allows the device to act as a “bump in the wire” and means that the device forwards all the network traffic it sees, regardless of its source and destination. You cannot disable this option on 7000 and 8000 Series devices.

Strict TCP Enforcement



Note Strict TCP enforcement is not supported on virtual devices. Only 7000 and 8000 Series devices support this option. In addition, you cannot enable this option and tap mode on the same inline set.

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

Configuring Advanced Inline Set Options

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to edit the inline set.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Inline Sets**.

Step 4 Click **Edit** ( ) next to the inline set you want to edit.

Step 5 Click **Advanced**.

Step 6 Configure options as described in Advanced Inline Set Options, on page 9.

Note Link state propagation and strict TCP enforcement are not supported on virtual devices.

Step 7 Click **OK**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Deleting Inline Sets

When you delete an inline set, any inline interfaces assigned to the set become available for inclusion in another set. The interfaces are not deleted.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to delete the inline set, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Inline Sets**.

Step 4 Next to the inline set you want to delete, click **Delete** ( ).

Step 5 When prompted, confirm that you want to delete the inline set.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.