Managing IPS Device Interface

Dedicated IPS appliances and service modules have their own interface configuration, whereas Cisco IOS IPS devices are configured using the regular router interface policies. This chapter explains how to configure interfaces for dedicated IPS appliances and service modules only.

This chapter contains the following topics:

Understanding Interfaces

Tip This topic is an overview of IPS interfaces. For more detailed information, including the specific interface names and locations for each type of appliance and service module, supported roles, configuration restrictions, and hardware considerations, refer to the "Configuring Interfaces" chapter of the Installing and Using Cisco Intrusion Prevention System Device Manager for the IPS software version you are using on Cisco.com. The information is also in the IME and CLI guidesFor general information, see http://www.cisco.com/go/ips.

The sensor interfaces are named according to the maximum speed and physical location of the interface. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom expansion slot.

There are three interface roles:

- **Command and control**—The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics.

The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface. See the IPS document cited above for a list of command and control interfaces by device type.

- **Sensing**—Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces. In promiscuous mode, packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic. In inline mode, the IPS

is in the traffic flow and can directly affect the traffic. For more information about sensing modes, see Understanding Interface Modes , on page 2.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled. See the IPS document cited above for a list of sensing interfaces by device type.

- **Alternate TCP reset**—You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode are instead sent out on the associated alternate TCP reset interface.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode (interface or VLAN pair), because TCP resets are always sent on the sensing interfaces in those modes.

Note With the exception of IDSM-2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on IDSM-2 is fixed because of hardware limitation. However, there is only one sensing interface on IPS modules (on routers or ASA devices), so you cannot specify an alternate TCP reset interface on them. See the IPS document cited above for a list of eligible alternate TCP reset interfaces by device type, and for more information about the conditions under which you would use one.

Understanding Interface Modes

Sensing interfaces can operate in various modes. The mode configured for an interface determines the traffic it can inspect and how it can respond to events.

This section contains the following topics:

Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous

mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline interface mode to promiscuous mode, delete any inline interface that contains that interface and delete any inline VLAN pair subinterfaces of that interface from the interface configuration.

Related Topics

- Understanding Interfaces , on page 1
- Configuring Physical Interfaces , on page 9

Inline Interface Mode

Operating in inline interface pair mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on Layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop or block attacks that would normally pass through a traditional firewall device.

In inline interface pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Notes:

- If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.
- You can configure IPS modules for routers and ASA devices to operate inline even though these modules have only one sensing interface.

Related Topics

- Understanding Interfaces , on page 1
- Configuring Inline Interface Pairs , on page 13

Inline VLAN Pair Mode

You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Notes:

- You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.
- Inline VLAN pairs are not supported on IPS modules for routers or ASA devices.

Related Topics

- Understanding Interfaces , on page 1
- Configuring Inline VLAN Pairs , on page 14

VLAN Group Mode

You can divide each physical interface or inline interface into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface. If you configure multiple virtual sensors, each of them can monitor one or more of these interfaces. This lets you apply multiple policies to the same sensor. The advantage is that now you can use a sensor with only a few interfaces as if it had many interfaces.

Note You cannot divide physical interfaces that are in inline VLAN pairs into VLAN groups.

VLAN group subinterfaces associate a set of VLANs with a physical or inline interface. No VLAN can be a member of more than one VLAN group subinterface. Each VLAN group subinterface is identified by a number between 1 and 255. Subinterface 0 is a reserved subinterface number used to represent the entire unvirtualized physical or logical interface. You cannot create, delete, or modify subinterface 0 and no statistics are reported for it.

When you create a VLAN group, it is either promiscuous or inline:

- Promiscuous VLAN group—If you configure a VLAN group on a physical interface, the VLAN group is promiscuous, as described in Promiscuous Mode , on page 2.
- Inline VLAN group—If you configure a VLAN group on an inline interface pair (a logical interface), the VLAN group is inline, as described in Inline Interface Mode , on page 3.

Thus, VLAN groups augment the operation of promiscuous mode interfaces or inline interfaces by confining their operation to selected VLANs. Once you assign a VLAN group to an interface (physical or inline interface), the interface is no longer a plain promiscuous or inline interface pair and can only be used for inline VLAN groups.

An unassigned VLAN group is maintained that contains all VLANs that are not specifically assigned to another VLAN group. You cannot directly specify the VLANs that are in the unassigned group. When a VLAN is added to or deleted from another VLAN group subinterface, the unassigned group is updated.

Packets in the native VLAN of an 802.1q trunk do not normally have 802.1q encapsulation headers to identify the VLAN number to which the packets belong. A default VLAN variable is associated with each physical interface and you should set this variable to the VLAN number of the native VLAN or to 0. The value 0 indicates that the native VLAN is either unknown or you do not care if it is specified. If the default VLAN setting is 0, the following occurs:

- Any alerts triggered by packets without 802.1q encapsulation have a VLAN value of 0 reported in the alert.
- Non-802.1q encapsulated traffic is associated with the unassigned VLAN group and it is not possible to assign the native VLAN to any other VLAN group.

Note You can configure a port on a switch as either an access port or a trunk port. On an access port, all traffic is in a single VLAN is called the access VLAN. On a trunk port, multiple VLANs can be carried over the port, and each packet has a special header attached called the 802.1q header that contains the VLAN ID. This header is commonly referred as the VLAN tag. However, a trunk port has a special VLAN called the native VLAN. Packets in the native VLAN do not have the 802.1q headers attached. IDSM-2 can read the 802.1q headers for all nonnative traffic to determine the VLAN ID for that packet. However, IDSM-2 does not know which VLAN is configured as the native VLAN for the port in the switch configuration, so it does not know what VLAN the native packets are in. Therefore, you must tell IDSM-2 which VLAN is the native VLAN for that port. Then IDSM-2 treats any untagged packets as if they were tagged with the native VLAN ID.

Related Topics

- Deploying VLAN Groups , on page 5
- Understanding Interfaces , on page 1
- Configuring VLAN Groups , on page 16

Deploying VLAN Groups

Because a VLAN group of an inline pair does not translate the VLAN ID, an inline paired interface must exist between two switches to use VLAN groups on a logical interface. For an appliance, you can connect the two pairs to the same switch, make them access ports, and then set the access VLANs for the two ports differently. In this configuration, the sensor connects between two VLANs, because each of the two ports is in access mode and carries only one VLAN. In this case the two ports must be in different VLANs, and the sensor bridges the two VLANs, monitoring any traffic that flows between the two VLANs. IDSM-2 also operates in this manner, because its two data ports are always connected to the same switch.

You can also connect appliances between two switches. There are two variations. In the first variation, the two ports are configured as access ports, so they carry a single VLAN. In this way, the sensor bridges a single VLAN between the two switches.

In the second variation, the two ports are configured as trunk ports, so they can carry multiple VLANs. In this configuration, the sensor bridges multiple VLANs between the two switches. Because multiple VLANs are carried over the inline interface pair, the VLANs can be divided into groups and each group can be assigned to a virtual sensor. The second variation does not apply to IDSM-2 because it cannot be connected in this way.

Related Topics

- Understanding Interfaces , on page 1
- VLAN Group Mode , on page 4
- Configuring VLAN Groups , on page 16

Configuring Interfaces

Use the Interfaces policy for IPS appliances and service modules to configure the interface settings for the device. The following topics explain how to configure the various types of settings. These topics do not apply to Cisco IOS IPS devices, which use the standard router interface policies.

- Understanding the IPS Interfaces Policy , on page 6
- Configuring Physical Interfaces , on page 9
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13
- Configuring Inline Interface Pairs , on page 13
- Configuring Inline VLAN Pairs , on page 14
- Configuring VLAN Groups , on page 16
- Viewing a Summary of IPS Interface Configuration , on page 8

Understanding the IPS Interfaces Policy

Use the Interfaces policy to configure the physical interfaces, inline pairs, VLAN pairs, and VLAN groups on IPS appliances and service modules. This policy does not apply to Cisco IOS IPS devices.

You can configure any single physical interface to run in promiscuous mode, inline pair mode, inline VLAN pair mode, promiscuous VLAN group, or inline VLAN group, but you cannot configure an interface in a combination of these modes.

Tip The contents of this policy differ depending on the device type and IPS software version. For example, some devices display the physical interfaces tab only; creating the other types of configurations is not supported. If a tab or option described below does not appear on the policy you are configuring, it does not apply to the device.

Navigation Path

(Device view only) Select **IPS** > **Interfaces** from the Policy selector.

Related Topics

- Understanding Interfaces , on page 1

- Understanding Interface Modes , on page 2
- Discovering Policies on Devices Already in Security Manager

Field Reference

Table 1: IPS Interfaces Policy

Element	Description
Physical Interfaces tab	The physical interfaces that are available on the device. You can edit these interfaces only (select the device and click the **Edit Row** button); you must perform inventory discovery on the device to obtain the correct list of physical interfaces, for example, if you add an interface card to the device. The columns displayed on the tab show the configuration of each interface and are explained in Modify Physical Interface Map Dialog Box , on page 10. Note that the Administrative State column indicates whether the interface is enabled (Yes or No); you must enable an interface for it to function. For more information, see Configuring Physical Interfaces , on page 9.
Inline Pairs tab	The inline interface pairs that allow inline mode processing, as described in Inline Interface Mode , on page 3. The table shows the name of the pair, the interfaces that are part it, and a description, if any. For more information, see Configuring Inline Interface Pairs , on page 13. • To add a pair, click the **Add Row** button and fill in the Add Interface Pair dialog box. • To edit a pair, select it and click the **Edit Row** button. • To delete a pair, select it and click the **Delete Row** button.
VLAN Pairs tab	The VLAN pairs for each physical interface, as described in Inline VLAN Pair Mode , on page 3. The table shows the interface and subinterface, with the two VLANs that are paired, and a description, if any. For more information, see Configuring Inline VLAN Pairs , on page 14. • To add a pair, click the **Add Row** button and fill in the Add VLAN Pair dialog box. • To edit a pair, select it and click the **Edit Row** button. • To delete a pair, select it and click the **Delete Row** button.
VLAN Groups tab	The VLAN groups defined for a physical interface or inline pair, as described in VLAN Group Mode , on page 4. The table shows the name of the interface or pair, the VLAN group (empty means all unassigned VLANs), and a description, if any. For more information, see Configuring VLAN Groups , on page 16. • To add a group, click the **Add Row** button and fill in the Add VLAN Group dialog box. • To edit a group, select it and click the **Edit Row** button. • To delete a group, select it and click the **Delete Row** button.

Element	Description
Summary tab	A summary of how you have configured the sensing interfaces—the interfaces you have configured for promiscuous mode, the interfaces you have configured as inline pairs, and the interfaces you have configured as inline VLAN pairs. For more information, see Viewing a Summary of IPS Interface Configuration , on page 8.
Bypass Mode	The bypass mode for the device, which determines how the sensor should handle inline mode traffic when the sensor processes are temporarily stopped for upgrades or when the sensor monitoring processes fail. This is a global setting that applies to all inline mode interfaces on the device. Select the desired option; for a detailed explanation of how each of these options affect inline traffic, see Configuring Bypass Mode , on page 12. • **Off (Always inspect inline traffic)**—Disables bypass mode. Traffic is always inspected, and if the monitoring process of the sensor is down, traffic stops flowing. • **On (Never inspect inline traffic)**—Traffic bypasses the Analysis Engine and is never inspected. • **Auto (Bypass inspection when analysis engine is stopped)**—Traffic is inspected unless the monitoring process of the sensor is down, in which case traffic continues to flow through the sensor uninspected. This is the default. Auto mode is useful during sensor upgrades to ensure that traffic is still flowing while the sensor is being upgraded.
CDP Mode	How to handle Cisco Discovery Protocol (CDP) packets. The CDP configuration applies globally to all interfaces on the device, however, it has an effect only on inline interfaces (both inline interfaces and inline VLAN pairs). For more information, see Configuring CDP Mode , on page 13. Select the desired option: • **Forward CDP packets**—To allow CDP packets to pass through the sensor. • **Drop CDP packets**—To have the sensor drop all CDP packets and not allow them to pass through the sensor. This is the default setting.

Viewing a Summary of IPS Interface Configuration

The Summary tab of the Interfaces policy contains a table summarizing how you have configured the sensing interfaces—the interfaces you have configured for promiscuous mode, the interfaces you have configured as inline pairs, the interfaces you have configured as inline VLAN pairs, inline VLAN groups, and promiscuous VLAN groups. The content of this table changes when you change your interface configuration.

You can configure any single physical interface to run in promiscuous mode, inline pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

Tip Not all service modules have a summary tab.

Navigation Path

(Device view) Select **Interfaces** from the Policy selector. Click the **Summary** tab.

Related Topics

- Understanding Interfaces , on page 1
- Understanding the IPS Interfaces Policy , on page 6
- Configuring Physical Interfaces , on page 9
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13
- Configuring Inline Interface Pairs , on page 13
- Configuring Inline VLAN Pairs , on page 14
- Configuring VLAN Groups , on page 16

Field Reference

Table 2: IPS Interface Summary Tab

Element	Description
Name	The name of the interface. The names are FastEthernet or GigabitEthernet for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
Subinterface Number	The subinterface number of the inline VLAN pair or VLAN group. Subinterface numbers can be from 1 to 255.
Inline Interface Name	The name of the inline interface pair.
Mode	The mode for the interface: promiscuous, inline, promiscuous VLAN group, or inline VLAN group and whether there are VLAN pairs. For an explanation of interface modes, see Understanding Interface Modes , on page 2.
VLAN A VLAN B	The VLAN ID for the first and second VLANs for VLAN pairs. VLAN numbers can be from 1 to 4095.
VLAN Range	The range of VLAN IDs belonging to the VLAN group, for example, 100-200. If the VLAN group is configured to apply to all unassigned VLANs, the field is empty.

Configuring Physical Interfaces

The Physical Interfaces tab of the IPS Interfaces policy lists the existing physical interfaces on your sensor and their associated settings. You cannot add or delete physical interfaces in this policy; instead, you must use policy discovery to obtain the current list of interfaces from the device. Thus, if you add or remove interface cards (available for some appliances), you must rediscover the device as described in Discovering Policies on Devices Already in Security Manager.

To configure the sensor to monitor traffic, you must enable the interface using this procedure. When you initialized the sensor using the **setup** command (using the command line interface on the IPS), you assigned

the interface or the inline pair to a virtual sensor, and enabled the interface or inline pair. If you need to change your interfaces settings, you can do so on the Physical Interfaces tab. To assign an interface to a virtual sensor, select the Virtual Sensors policy and add or edit the virtual sensor, as appropriate.

Tip Each physical interface can be divided into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface. For more information, see Configuring VLAN Groups , on page 16.

Related Topics

- Understanding Interfaces , on page 1
- Defining A Virtual Sensor
- Editing Policies for a Virtual Sensor
- Assigning Interfaces to Virtual Sensors
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13
- Configuring Inline Interface Pairs , on page 13

Step 1 (Device view) Select **Interfaces** from the Policy selector, then click the **Physical Interfaces** tab (if necessary).

Step 2 Select the interface whose configuration you want to change and click the **Edit Row** button. The Modify Physical Interface Map dialog box appears.

Step 3 Make the desired configuration changes and click **OK**. Following are the settings you are most likely to want to change; for a description of all options, see Modify Physical Interface Map Dialog Box , on page 10.

- **Enabled**—Whether the interface is enabled (**Yes** or **No**). Select Yes to make the interface functional. The value of this option is shown in the Administrative State column in the Physical Interfaces tab.
- **Default VLAN**—The VLAN to which the interface is assigned.
- **Specify Interface for TCP Reset**—If you want to assign an alternate TCP reset interface, as described in Understanding Interfaces , on page 1, select this option, then select the alternate interface from the **interface-name** list.

Modify Physical Interface Map Dialog Box

Use the Modify Physical Interface Map dialog box to change the configuration of the physical interfaces of an IPS sensor. For the procedure, see Configuring Physical Interfaces , on page 9.

Navigation Path

(Device view) Select **Interfaces** from the Policy selector. On the **Physical Interfaces** tab, select an interface and click the **Edit Row** button.

Related Topics

- Understanding Interfaces , on page 1
- Understanding the IPS Interfaces Policy , on page 6

Field Reference

Table 3: Modify Physical Interface Map Dialog Box

Element	Description
Name	The name of the physical interface.
Media Type	The type of media for the physical interface. The media types are the following: • TX—Copper media. • SX—Fiber media. • XL—Network accelerator card. • Backplane interface—An internal interface that connects the module to the backplane of the parent chassis.
Description	A description of the interface.
Enabled	Whether the interface is enabled, Yes or No. You must select **Yes** for the interface to be functional. You also have to assign the interface to a virtual sensor for it to monitor traffic; use the Virtual Sensors policy.
Duplex	The duplex setting of the interface. The duplex types are the following: • Auto—Sets the interface to auto negotiate duplex. • Full—Sets the interface to full duplex. • Half—Sets the interface to half duplex.
Speed	The speed setting of the interface. The speed options are the following: • Auto—Sets the interface to auto negotiate speed. • 10 MB—Sets the interface to 10 MB (for TX interfaces only). • 100 MB—Sets the interface to 100 MB (for TX interfaces only). • 1 GB—Sets the interface to 1 GB (for gigabit interfaces only). • 10 GB—Sets the interface to 10 GB (for 10 gigabit interfaces only).
Default VLAN	The VLAN ID associated with native traffic, or 0 if unknown or if you do not care which VLAN it is.

Element	Description
Specify Interface for TCP Reset interface-name	Whether to send TCP resets on an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing. If you select this option, select the alternate TCP reset interface from the interface-name list. For more information about alternate TCP reset, see Understanding Interfaces , on page 1.

Configuring Bypass Mode

You can use inline bypass as a diagnostic tool and a failover protection mechanism. Normally, the sensor Analysis Engine performs packet analysis. When inline bypass is activated, Analysis Engine is bypassed, allowing traffic to flow through the inline interfaces and inline VLAN pairs without inspection. Inline bypass ensures that packets continue to flow through the sensor when the sensor processes are temporarily stopped for upgrades or when the sensor monitoring processes fail. There are three modes: on, off, and automatic. By default, bypass mode is set to automatic.

Keep the following factors in mind before deciding which bypass mode to use:

- There are security consequences when you put the sensor in bypass mode. When bypass mode is on, the traffic bypasses the sensor and is not inspected; therefore, the sensor cannot prevent malicious attacks.
- The inline bypass functionality is implemented in software, so it functions only when the operating system is running. If the sensor is powered off or shut down, inline bypass does not work—traffic does not flow through the sensor.
- When the sensor applies a signature or global correlation update, it might trigger bypass. Whether bypass is triggered depends on the traffic load of the sensor and the size of the signature or global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

To change the bypass mode setting, follow these steps:

Step 1 (Device view) Select the **Interfaces** policy from the Policy selector.

Step 2 In the **Bypass Mode** field at the bottom of the policy, select the desired option:

- **Off (Always inspect inline traffic)**—Disables bypass mode.

Traffic flows through the sensor for inspection. If the monitoring process of the sensor is down, traffic stops flowing. This means that inline traffic is always inspected.

- **On (Never inspect inline traffic)**—Traffic bypasses the Analysis Engine and is not inspected. This means that inline traffic is never inspected.
- **Auto (Bypass inspection when analysis engine is stopped)**—Traffic flows through the sensor for inspection unless the monitoring process of the sensor is down. This is the default.

If the monitoring process of the sensor is down, traffic bypasses the sensor until the sensor is running again. The sensor then inspects the traffic. Auto mode is useful during sensor upgrades to ensure that traffic is still flowing while the sensor

is being upgraded. Auto mode also helps to ensure traffic continues to pass through the sensor if the monitoring process fails.

Configuring CDP Mode

You can configure the IPS sensor to enable or disable the forwarding of Cisco Discovery Protocol (CDP) packets. The CDP configuration applies globally to all interfaces on the device, however, it has an effect only on inline interfaces (both inline interfaces and inline VLAN pairs).

Cisco Discovery Protocol is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.

Tip The CDP Mode setting is not available on all IPS appliances and service modules. If the CDP Mode field does not appear on the Interfaces policy, the setting does not apply to the device you are configuring.

To change the CDP mode setting on a device, follow these steps:

Step 1 (Device view) Select the **Interfaces** policy from the Policy selector.

Step 2 In the **CDP Mode** field at the bottom of the policy, select the desired option:

- **Forward CDP packets**—To allow CDP packets to pass through the sensor.
- **Drop CDP packets**—To have the sensor drop all CDP packets and not allow them to pass through the sensor. This is the default setting.

Configuring Inline Interface Pairs

You can pair interfaces on your sensor if your sensor is capable of inline monitoring. For more information about inline pairs, see Inline VLAN Pair Mode , on page 3.

Tip IPS modules for routers and ASA devices do not need an inline pair for monitoring. You only need to add the physical interface to a virtual sensor.

Related Topics

- Understanding Interfaces , on page 1
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13

- Configuring Physical Interfaces , on page 9
- Configuring VLAN Groups , on page 16
- Defining A Virtual Sensor
- Editing Policies for a Virtual Sensor
- Assigning Interfaces to Virtual Sensors

Step 1 (Device view) Select **Interfaces** from the Policy selector, then click the **Inline Pairs** tab.

Step 2 Do one of the following:

- To add a pair, click the **Add Row** button. The Add Interface Pair dialog box opens.
- To edit a pair, select it and click the **Edit Row** button. The Edit Interface Pair dialog box opens.

Tip You can also delete a pair by selecting it and clicking the **Delete Row** button. You cannot delete an inline pair if there is an inline VLAN group. First delete the inline VLAN group from the VLAN Groups tab, and then delete the inline pair.

Step 3 In the Add or Edit Inline Pairs dialog box, configure the following options:

- **Inline Interface Name**—The name you want to give to this inline pair. The name cannot be longer than 32 characters; alphanumeric and underscore characters are allowed. You cannot edit this name after you create the pair.
- **Interface 1 and 2**—Select the two physical interfaces that you want to form a pair. The lists include only those interfaces that are defined on the Physical Interfaces tab and that are not already part of an inline pair, VLAN pair, or VLAN group.
- **Description**—An optional description for the pair.

Step 4 Click **OK** to save your changes.

Configuring Inline VLAN Pairs

Use the VLAN Pairs tab of the IPS Interfaces policy to configure the VLAN pairs for physical interfaces. The summary table displays the existing VLAN pairs for each physical interface. You can create multiple VLAN pairs on a single physical interface. For more information about inline VLAN pair mode, see Inline VLAN Pair Mode , on page 3.

Tips

- You cannot create a VLAN pair for an interface if it is already part of an inline interface pair; create VLAN groups for inline interface pairs.
- To create an inline VLAN pair for an interface that is in promiscuous mode and assigned to a virtual sensor, you must first remove the interface from the virtual sensor (using the Virtual Sensors policy) and then create the inline VLAN pair.
- You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

- If your sensor does not support inline VLAN pairs, the VLAN Pairs pane is not displayed. IPS modules on routers and ASA devices do not support inline VLAN pairs.
- When using inline VLAN pairs, you should configure UniDirectional Link Detection (UDLD) on the connected switch that is hosting the VLANs. UDLD can help switches prevent spanning-tree forwarding loops and single direction links. For detailed information, see https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/idm/idmguide7/idm_interfaces.html#wp1169508

Related Topics

- Understanding Interfaces , on page 1
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13
- Configuring Physical Interfaces , on page 9
- Configuring VLAN Groups , on page 16

Step 1 (Device view) Select **Interfaces** from the Policy selector, then click the **VLAN Pairs** tab.

Step 2 Do one of the following:

- To add a pair, click the **Add Row** button. The Add VLAN Pair dialog box opens.
- To edit a pair, select it and click the **Edit Row** button. The Edit VLAN Pair dialog box opens.

Tip You can also delete a pair by selecting it and clicking the **Delete Row** button. You cannot delete an inline VLAN pair if it is assigned to a virtual sensor. First remove the assignment to the virtual sensor using the Virtual Sensors policy, and then delete the inline VLAN pair.

Step 3 In the Add or Edit VLAN Pairs dialog box, configure the following options:

- **Physical Interfaces**—Select the physical interface on which you are creating this VLAN pair. The list includes only those interfaces that are defined on the Physical Interfaces tab and that are not already part of an inline interface pair or VLAN group. However, you can create multiple VLAN pairs on a single interface.
- **Subinterface Number**—Enter a number to assign as a subinterface. The number must be unique on the interface, that is, it cannot already be assigned to another VLAN pair on the selected physical interface. Subinterface numbers can be from 1 to 255.
- **Description**—An optional description for the pair.
- **VLAN A, B**—The numbers of the two VLANs that you want to join as a pair. VLAN numbers are from 1 to 4095. You must enter different numbers, and the numbers must not already be part of another VLAN pair on the selected physical interface.

Step 4 Click **OK** to save your changes.

Configuring VLAN Groups

Use the VLAN Groups tab of the IPS Interfaces policy to configure the VLAN groups for physical interfaces and inline interface pairs (logical interfaces). The summary table displays the existing VLAN groups. You can create multiple VLAN groups on a single physical interface or inline interface pair. For more information about VLAN group mode, see VLAN Group Mode , on page 4.

A VLAN group consists of a group of VLAN IDs that exist on an interface. Each VLAN group consists of at least one VLAN ID. You can have up to 255 VLAN groups per interface (logical or physical). Each group can contain any number of VLAN IDs.

After you assign the VLAN IDs to the VLAN group, you must assign the VLAN group to a virtual sensor for it to be operational. You can assign a single group to at most one virtual sensor. Use the Virtual Sensors policy to make the assignment.

Note VLAN groups are supported in IPS 6.0 and later only. Not all IPS appliances or service modules support VLAN groups. If the VLAN Groups tab does not appear in the Interfaces policy, the device you are configuring does not support the feature.

Related Topics

- Understanding Interfaces , on page 1
- Configuring Bypass Mode , on page 12
- Configuring CDP Mode , on page 13
- Configuring Physical Interfaces , on page 9
- Defining A Virtual Sensor
- Editing Policies for a Virtual Sensor
- Assigning Interfaces to Virtual Sensors

Step 1 (Device view) Select **Interfaces** from the Policy selector, then click the **VLAN Groups** tab.

The table shows the existing VLAN groups, including the interface for which the group is defined, the subinterface number, description (if any), and the VLANs assigned to the group. If the VLANs cell is empty, the group is defined for all unassigned VLANs on the interface.

Step 2 Do one of the following:

- To add a pair, click the **Add Row** button. The Add VLAN Group dialog box opens.
- To edit a pair, select it and click the **Edit Row** button. The Edit VLAN Group dialog box opens.

Tip You can also delete a group by selecting it and clicking the **Delete Row** button. You cannot delete a VLAN group if it is assigned to a virtual sensor. First remove the assignment to the virtual sensor using the Virtual Sensors policy, and then delete the VLAN group.

Step 3 In the Add or Edit VLAN Group dialog box, configure the following options:

- **Physical and Logical Interfaces**—Select the physical interface or inline interface pair for which you are creating this VLAN group. The list includes only unpaired physical interfaces (defined on the Physical Interfaces tab) that do not already have inline VLAN pairs defined, or inline interface pairs that are defined on the Inline Pairs tab. You can create multiple VLAN groups on a single interface. Keep the following in mind:
  - If you select a physical interface, you are creating a promiscuous VLAN group.
  - If you select a logical interface, you are creating an inline VLAN group.
- **Subinterface Number**—Enter a number to assign as a subinterface. The number must be unique on the interface, that is, it cannot already be assigned to another VLAN group on the selected interface. Subinterface numbers can be from 1 to 255.
- **Description**—An optional description for the group.
- VLAN assignment—Select one of the following options:
  - **All Unassigned VLAN IDs**—The group contains all VLANs that are not assigned to other VLAN groups. This is the default option
  - **Range of free VLAN IDs**—The group contains specific VLANs. In the **Range** box, enter any combination of single VLAN IDs or ranges (separate starting and ending ID with a hyphen), and separate multiple entries with commas. For example, 10, 12-25, 33-49. VLAN numbers are from 1 to 4095.

The VLAN ID cannot already be in another VLAN group for the selected interface. The VLANs also must be configured on the connected switch or there will be no traffic to inspect.

Step 4 Click **OK** to save your changes.