Configuring Virtual Sensors

All IPS devices and service modules have a base virtual sensor named vs0. When you configure the IPS appliance or service module, you must configure the base vs0 sensor to assign interfaces to it. This assignment tells the device which interfaces to inspect. There are also other settings that are configured on virtual sensors.

In addition to the base vs0 virtual sensor, many IPS appliances and service modules allow you to create user-defined virtual sensors. You can use these virtual sensors to create separate policies for traffic, so that a single physical sensor can act as if it were multiple sensors. A virtual sensor is a logical grouping of sensing interfaces and the configuration policy for the signature engines and event action filters to apply.

This chapter contains the following topics:

- Understanding the Virtual Sensor , on page 1
- Defining A Virtual Sensor , on page 5
- Editing Policies for a Virtual Sensor , on page 9
- Deleting A Virtual Sensor , on page 10

Understanding the Virtual Sensor

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall, from behind the firewall, or from in front of and behind the firewall concurrently. A single sensor can monitor one or more data streams. In this situation a single sensor policy or configuration is applied to all monitored data streams.

With virtual sensors, you can create separate policies to apply to specific traffic feeds. For example, if you want to create a policy for a data center and a second much different policy for the campus network, yet run both policies on the same hardware device, you can configure separate virtual sensors to implement these policies.

You configure the following policies and settings separately for a virtual sensor:

- Signature and signature settings (policies in the IPS > Signatures folder).
- Event action policies (policies in the IPS > Event Actions folder).
- Anomaly detection policies (the IPS > Anomaly Detection policy) and the anomaly detection mode (in the Virtual Sensors policy).
- The promiscuous interfaces, inline interface pairs, inline VLAN pairs, inline VLAN groups, or promiscuous VLAN groups that the virtual sensor monitors.

Note No packet is processed by more than one virtual sensor; you cannot assign the same physical or logical interface to more than one sensor. Packets from interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups that are not assigned to any virtual sensor are disposed of according to the inline bypass configuration that you define in the **Interfaces** policy.

- The inline TCP session tracking and Normalizer modes (in the Virtual Sensors policy).

Note If you create a policy instance on an IPS device for signatures, event actions, or anomaly detection but do not assign it to any of the virtual sensors on that device (that is, you do not use that policy instance), then that policy instance is deleted by Security Manager during deployment.

All other policies and settings are configured on the parent device that hosts the virtual sensor. For example, if you want to use global correlation, you configure it on the parent device and the virtual sensors share that configuration.

You can configure up to four virtual sensors on one appliance, but you can add only three user-defined virtual sensors. The first virtual sensor, vs0, is the base sensor and you cannot delete it. In Security Manager, virtual sensors are presented as follows:

- The device selector in Device view contains the parent device, which doubles as the base virtual sensor, vs0. Select this device to configure all device-level policies and to create virtual sensors in the Virtual Sensors policy.
- Any user-defined virtual sensors are also shown in the device selector in Device view. The display name of the real device is prepended to the beginning of the name of the virtual sensor. In most cases, the result is that the virtual sensors appear next to the parent (real) device that the virtual sensor is on. For example, on the host (real device) named “bob,” the virtual sensor with the name “vs1” will appear in the device list as “bob_vs1.”

To configure the signature, anomaly detection, and event action policies for a virtual sensor, you must select it in the device selector. You cannot configure these policies by selecting the parent device; those policies on the parent device are for the vs0 base sensor.

The following topics explain more about virtual sensors:

- Advantages and Restrictions of Virtualization , on page 3
- Inline TCP Session Tracking Mode , on page 4
- Understanding Normalizer Mode , on page 4
- Assigning Interfaces to Virtual Sensors , on page 4
- Identifying the Virtual Sensors for a Device , on page 5
- Defining A Virtual Sensor , on page 5
- Editing Policies for a Virtual Sensor , on page 9
- Deleting A Virtual Sensor , on page 10

Advantages and Restrictions of Virtualization

An advantage of using virtual sensors is that you can operate more than one virtual sensor on one appliance while configuring each virtual sensor differently with regard to signature behavior and traffic feed. For example, if you want to create a policy for a data center and a second much different policy for the campus network, yet run both policies on the same hardware device, you can configure separate virtual sensors to implement these policies.

Virtualization has the following advantages:

- You can apply different configurations to different sets of traffic.
- You can monitor two networks with overlapping IP spaces with one sensor.
- You can monitor both inside and outside a firewall or NAT device.

Virtualization has the following restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- Using VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
  - When using Cisco IOS software, a VACL capture port or a SPAN target does not always receive tagged packets even if it is configured for trunking.
  - When using the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.
- Not all IPS sensors support multiple virtual sensors. The Virtual Sensors policy appears for all IPS appliances and service modules, because you must use it to assign interfaces to the base vs0 sensor. If the Add button in the policy is disabled for a device, and you have not configured user-defined virtual sensors, then the device does not support virtualization. Examples of devices that do not support virtualization include the Cisco IPS 4215, NM-CIDS, AIM-IPS, NME-IPS, and AIP-SSC. IDSM2 supports virtualization, but it does not support VLAN groups or inline interface pairs.
- You must use IPS 6.0+ software. Older software versions do not support virtualization.
- Cisco IOS IPS devices do not support virtualization. Use the **IPS > Interface Rules** policy to specify the interfaces that IPS should monitor.

Virtualization has the following traffic capture requirements:

- The virtual sensor must receive traffic that has 802.1q headers (other than traffic on the native VLAN of the capture port).
- The sensor must see both directions of traffic in the same VLAN group in the same virtual sensor for any given sensor.

Related Topics

- Understanding the Virtual Sensor , on page 1
- Defining A Virtual Sensor , on page 5

Inline TCP Session Tracking Mode

When you choose to modify packets inline, if the packets from a stream are seen twice by the Normalizer engine, it cannot properly track the stream state and often the stream is dropped. This situation occurs most often when a stream is routed through multiple VLANs or interfaces that are being monitored by the IPS. A further complication in this situation is the necessity of allowing asymmetric traffic to merge for proper tracking of streams when the traffic for either direction is received from different VLANs or interfaces.

To deal with this situation, you can set the mode so that streams are perceived as unique if they are received on separate interfaces or VLANs (or the subinterface for VLAN pairs).

The following inline TCP session tracking modes apply:

- **Interface and VLAN**—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
- **VLAN Only**—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately.
- **Virtual Sensor**—All packets with the same session key (AaBb) within a virtual sensor belong to the same session. This is the default and almost always the best option to choose.

You configure the inline TCP session tracking mode as a property of the virtual sensor as described in Defining A Virtual Sensor , on page 5.

Understanding Normalizer Mode

Normalizer mode applies only when the sensor is operating in inline mode. The default is strict evasion protection, which is full enforcement of TCP state and sequence tracking. The Normalizer enforces duplicate packets, changed packets, out-of-order packets, and so forth, which helps prevent attackers from evading the IPS.

Asymmetric mode disables most of the Normalizer checks. Use Asymmetric mode only when the entire stream cannot be inspected, because in this situation, attackers can now evade the IPS.

You configure the Normalizer mode as a property of the virtual sensor as described in Defining A Virtual Sensor , on page 5.

Assigning Interfaces to Virtual Sensors

An IPS sensor monitors traffic that traverses interfaces, interface pairs, or VLAN pairs assigned to a virtual sensor.

You can assign one or more of the following types of interfaces to a virtual sensor:

- Promiscuous interface—A physical interface that does not have VLAN groups and which is not part of an inline interface pair.
- Inline interface pair—A logical interface composed of two physical interfaces.
- Inline VLAN pair—A logical interface composed of two VLANs.
- Promiscuous VLAN group—A VLAN group that is assigned to a subinterface on a physical interface.

The physical interface cannot already be used for an inline interface or VLAN pair. There can be many promiscuous VLAN groups on the same promiscuous interface, but the VLANs assigned cannot overlap. Once a VLAN group is assigned to a promiscuous interface, it is no longer a plain promiscuous interface and can only be used for promiscuous VLAN groups.

- Inline VLAN group—A VLAN group that is assigned to a subinterface of an inline interface pair.

There can be many inline VLAN groups on the same inline interface pair, but the VLANs assigned cannot overlap. Once a VLAN group is assigned to an inline interface pair it is no longer a plain inline interface pair and can only be used for inline VLAN groups.

VLAN groups cannot be assigned to inline VLAN pairs.

You must configure the interfaces before you can assign them to virtual sensors. For more information about configuring all of these types of interfaces, see Configuring Interfaces. For information on assigning interfaces to virtual sensors, see Defining A Virtual Sensor , on page 5.

Identifying the Virtual Sensors for a Device

If you configure user-defined virtual sensors on an IPS appliance or service module, the virtual sensor appears in the device selector in Device view.

Normally, the display name of a virtual sensor is in the form *device-name_virtual-sensor-name* , where *device-name* is the name of the parent device, and *virtual-sensor-name* is the name of the virtual sensor. For example, the virtual sensor vs1 on device 10.100.10.10 would be 10.100.10.10_vs1.

Thus, under normal conditions, the virtual sensors for a device should appear immediately after the parent device in the device selector. However, you can change the virtual sensor's display name by editing the device properties. If you alter the default name, the virtual sensors might not appear anywhere near the parent device in the device selector.

You can use the following techniques to identify the virtual sensors defined on a device, or to identify the parent device of a virtual sensor:

- To see a list of virtual sensors defined on an IPS device, select the **Virtual Sensors** policy on the device. The table shows all virtual sensors, including the base vs0 sensor. Note that the vs0 sensor does not appear separately in the device selector; it is represented by the parent device itself.

Unless you radically alter the display names of virtual sensors, the virtual sensor name, along with the parent device's display name, should help you find the virtual sensor in the device selector.

- To determine which IPS device is the host of a virtual sensor, right-click the virtual sensor in the device selector and select **Device Properties**. The Hostname display-only field on the General tab shows the host device display name plus the virtual sensor name as defined on the device.

Defining A Virtual Sensor

Use the Virtual Sensors policy to configure virtual sensors on your Cisco IPS devices. Even if your IPS device does not support multiple virtual sensors, you must use this policy to assign interfaces to the base sensor, vs0, and configure properties that are associated with the virtual sensor.

Tip For Cisco IOS IPS devices, you configure the interfaces that the IPS examines in the **IPS > Interface Rules** policy. You cannot configure virtual sensors in an IOS IPS device.

Before You Begin

Configure the interfaces on the sensor, including inline interface pairs, inline VLAN pairs, and promiscuous and inline VLAN groups. The interface configurations must exist before you can assign them to a virtual sensor. For information on interfaces, interface modes, and how to configure them, see Managing IPS Device Interface.

Related Topics

- Understanding Interfaces
- Understanding Interface Modes
- Advantages and Restrictions of Virtualization , on page 3
- Inline TCP Session Tracking Mode , on page 4
- Inline TCP Session Tracking Mode , on page 4
- Understanding Normalizer Mode , on page 4
- Assigning Interfaces to Virtual Sensors , on page 4
- Identifying the Virtual Sensors for a Device , on page 5
- Editing Policies for a Virtual Sensor , on page 9

Procedure

Step 1 (Device view only.) Select **Virtual Sensors** from the Policies selector to open the Virtual Sensors policy.

The policy lists all existing virtual sensors, including the base vs0 sensor, which you cannot delete. The information for each sensor shows the interfaces assigned to the sensor, anomaly detection mode, inline TCP tracking mode, normalizer mode, and a description, if any. If the Assignments cell is empty, no interfaces are assigned to the virtual sensor, which means the virtual sensor cannot analyze any traffic.

Step 2 Do one of the following:

- To add a virtual sensor, click the **Add Row** button. The Add Virtual Sensor dialog box opens.

You can add at most three sensors. The device supports four virtual sensors, including the base vs0 sensor. If the Add Row button is disabled, you either have configured the maximum number of sensors, or your device does not support multiple virtual sensors.

- To edit a virtual sensor, select it and click the **Edit Row** button. The Edit Virtual Sensor dialog box opens.

Tip You can also delete a virtual sensor by selecting it and clicking the **Delete Row** button. You cannot delete the base vs0 sensor. For more information about deleting virtual sensors, see Deleting A Virtual Sensor , on page 10.

Step 3 In the Add or Edit Virtual Sensor dialog box, configure at least the following options. The defaults for the other options are appropriate in most cases. For detailed information on all available options, see Virtual Sensor Dialog Box , on page 7.

- Virtual Sensor Name—The name of the virtual sensor. The virtual sensor name can be up to 64 characters and it cannot contain spaces.
- Interface assignments (Available, Assigned lists)—The promiscuous interfaces, inline interface pairs, inline VLAN pairs, promiscuous VLAN groups, or inline VLAN groups that you want this virtual sensor to use. The list of available interfaces shows only those interfaces that are configured in the Interfaces policy and that are not yet assigned to another virtual sensor.
  - To assign interfaces, select them in the available list and click >>.
  - To remove an assignment, select the interface in the assigned list and click <<. You must remove an assignment before you can assign an interface to a different virtual sensor.

Tip: If you are not sure about the content of a specific interface, for example, its mode or assigned VLANs, close the dialog box, go to the Interfaces policy, and examine the various tabs.

Step 4 Click **OK** to save your changes and add them to the Virtual Sensors policy.

Step 5 Click **Save** to save the Virtual Sensors policy.

Step 6 If you created a new virtual sensor, you must submit your changes to the database for the new virtual sensor to appear in the device selector in Device view.

- Non-Workflow mode—Select **File > Submit**.
- Workflow mode—Select **Activities > Approve Activity**, or if you are operating with an activity approver, **Activities > Submit Activity**. The activity must be approved before the virtual sensor appears in the device selector.

Note In the device selector, the display name of the real device is prepended to the beginning of the name of the virtual sensor. In most cases, the result is that the virtual sensors appear next to the parent (real) device that the virtual sensor is on. For example, on the host (real device) named “bob,” the virtual sensor with the name “vs1” will appear in the device list as “bob_vs1.”

Step 7 To configure the policies associated with a virtual sensor, select it in the device selector in Device view. You can then configure the associated policies. See the following topics:

- Defining IPS Signatures
- Configuring Event Action Rules
- Configuring Anomaly Detection Signatures

Virtual Sensor Dialog Box

Use the Add or Edit Virtual Sensor dialog box to configure the properties for a virtual sensor.

Navigation Path

(Device view only.) Select **Virtual Sensors** from the Policy selector. Click the **Add Row** button, or select an existing virtual sensor and click the **Edit Row** button.

Related Topics

- Defining A Virtual Sensor , on page 5
- Advantages and Restrictions of Virtualization , on page 3
- Assigning Interfaces to Virtual Sensors , on page 4
- Managing IPS Device Interface
- Understanding Interfaces
- Understanding Interface Modes

Field Reference

Table 1: Add or Edit Virtual Sensor Dialog Box

Element	Description
Virtual Sensor Name	The name of the virtual sensor. The virtual sensor name can be up to 64 characters and it cannot contain spaces. The name of the default virtual sensor is **vs0**. You cannot change the name after you create the virtual sensor. To change a virtual sensor name, delete the sensor and create a new sensor with the desired name. If you already configured local policies for the sensor (that is, signature, event action, and anomaly detection policies), first save the policies as shared policies, delete the sensor, create the new sensor, then assign the shared policies to the new virtual sensor. For more information about creating shared policies from local policies, see Sharing a Local Policy.
Interface Assignments (Available, Assigned)	The promiscuous interfaces, inline interface pairs, inline VLAN pairs, promiscuous VLAN groups, or inline VLAN groups that you want this virtual sensor to use. The list of available interfaces shows only those interfaces that are configured in the Interfaces policy and that are not yet assigned to another virtual sensor. • To assign interfaces, select them in the available list and click >>. • To remove an assignment, select the interface in the assigned list and click <<. You must remove an assignment before you can assign an interface to a different virtual sensor. **Tip** If you are not sure about the content of a specific interface, for example, its mode or assigned VLANs, close the dialog box, go to the Interfaces policy, and examine the various tabs.
Anomaly Detection Mode	The mode that you want the anomaly detection policy to operate in for this virtual sensor: Detect, Inactive, Learn. The default and normal operational mode is Detect. However, if you are using asymmetric normalizer mode, you might want to set the anomaly detection mode to Inactive. For detailed information about these modes, see Anomaly Detection Modes.

Element	Description
Inline TCP Session Tracking Mode	The mode used to segregate multiple views of the same stream if the same stream passes through the sensor more than once. The default mode is Virtual Sensor. For more information, see Inline TCP Session Tracking Mode , on page 4. Select one of the following: • Interface and VLAN—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) and on the same interface belong to the same session. Packets with the same key but on different VLANs are tracked separately. • VLAN Only—All packets with the same session key (AaBb) in the same VLAN (or inline VLAN pair) regardless of the interface belong to the same session. Packets with the same key but on different VLANs are tracked separately. • Virtual Sensor—All packets with the same session key (AaBb) within a virtual sensor belong to the same session.
Normalizer Mode	The type of Normalizer mode you need for traffic inspection. For more information, see Understanding Normalizer Mode , on page 4. • Strict Evasion Protection—(Default) If a packet is missed for any reason, all packets after the missed packet are not processed. Strict evasion protection provides full enforcement of TCP state and sequence tracking. Any out-of-order packets or missed packets can produce Normalizer engine signatures 1300 or 1330 firings, which try to correct the situation, but can result in denied connections. • Asymmetric Mode Protection—Can only see one direction of bidirectional traffic flow. Asymmetric mode protection relaxes the evasion protection at the TCP layer. Asymmetric mode lets the sensor synchronize state with the flow and maintain inspection for those engines that do not require both directions. Asymmetric mode lowers security because full protection requires both sides of traffic to be seen.
Description	The description of the virtual sensor.

Editing Policies for a Virtual Sensor

Virtual sensors have two types of policies: the virtual sensor's properties, and policies assigned to the virtual sensor. You use a different approach to edit these items.

- To edit the properties of a virtual sensor, select the virtual sensor's parent device in the device selector in Device view. Then, select the **Virtual Sensors** policy. You can then select the virtual sensor in the table and click the **Edit Row** button.

Using the Virtual Sensors policy, you can change the interfaces assigned to a sensor, the anomaly detection mode, inline TCP session tracking mode, and Normalizer mode. For more information, see the following topics:

- Defining A Virtual Sensor , on page 5

- Virtual Sensor Dialog Box , on page 7
- To edit the policies assigned to a virtual sensor, select the virtual sensor in the device selector in Device view. A virtual sensor's name is in the form *device-name_virtual-sensor-name* , where *device-name* is the name of the parent device, and *virtual-sensor-name* is the name of the virtual sensor. For example, the virtual sensor vs1 on device 10.100.10.10 would be 10.100.10.10_vs1.

Note The base virtual sensor, vs0, is integrated with the parent device and does not appear separately in the device selector. To configure the base virtual sensor, select the parent device.

You can then select the policies in the Policies selector and configure them. For more information, see the following topics:

- Defining IPS Signatures
- Configuring Event Action Rules
- Configuring Anomaly Detection

All other policies are configured on the parent device, and the configurations apply to all virtual sensors configured on the device.

Deleting A Virtual Sensor

Virtual sensors appear in the device selector in Device view. However, you cannot delete them from the selector using the same command used for other devices. Instead, you must delete the virtual sensor from the Virtual Sensors policy of the parent device, that is, the device on which the virtual sensor is defined. The following procedure explains how to delete a user-defined virtual sensor.

Tip The base virtual sensor, vs0, does not appear in the device selector. Instead, it is represented by the parent IPS sensor; it is considered to be the base IPS device. To delete the base vs0 sensor, you delete the entire device from the inventory. For information on deleting devices from the inventory, see Deleting Devices from the Security Manager Inventory.

Before You Begin

When you delete a virtual sensor, you also delete the policies defined for the sensor, such as signature, event action, and anomaly detection policies. If you configured non-default local policies, and you want to preserve them for use on other virtual sensors, you must first convert the local policies to shared policies. Then, after you delete the virtual sensor, the policies continue to exist as unassigned shared policies. You can then assign them to another virtual sensor. For more information on creating a shared policy from a local policy, see Sharing a Local Policy.

Using this technique is ideal if you are deleting a virtual sensor simply as a means to change the virtual sensor's name. Because you cannot change a virtual sensor's name, you must delete it and create a new virtual sensor with the desired name. If you created shared policies, you could then assign those shared policies to your new sensor, and it will have the same configuration as the sensor had under the old name.

Procedure

Step 1 (Device view only.) Select **Virtual Sensors** from the Policies selector to open the Virtual Sensors policy.

Step 2 Select the user-defined virtual sensor that you want to delete and click the **Delete Row** button.

Step 3 You are asked for a two-step confirmation. First, you are warned that you must save the policy to keep the policy and device synchronized. Click **OK** to continue, and you are also asked to confirm that you want to delete the node.

If you confirm, the virtual sensor is removed from both the policy and the device selector. It will take a few moments before the device view is updated and the virtual sensor disappears from the list of devices.