



CHAPTER 4

Configuring Virtual Sensors

This chapter explains the function of the Analysis Engine and how to create, edit, delete virtual sensors. It also explains how to assign interfaces to a virtual sensor. It contains the following sections:

- [Understanding Analysis Engine, page 4-1](#)
- [Understanding the Virtual Sensor, page 4-1](#)
- [Advantages and Restrictions of Virtualization, page 4-2](#)
- [Inline TCP Session Tracking Mode, page 4-3](#)
- [Configuring the Virtual Sensor, page 4-3](#)
- [Configuring Global Variables, page 4-7](#)

Understanding Analysis Engine

Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces.

You create virtual sensors in Analysis Engine. Each virtual sensor has a unique name with a list of interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups associated with it. To avoid definition ordering issues, no conflicts or overlaps are allowed in assignments—you assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a specific virtual sensor so that no packet is processed by more than one virtual sensor. Each virtual sensor is also associated with a specifically named signature definition, event action rules, and anomaly detection configuration. 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.



Note

IPS 6.0 does not support more than four virtual sensors. You cannot delete the default virtual sensor vs0.

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. And 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.

A virtual sensor is a collection of data that is defined by a set of configuration policies. The virtual sensor is applied to a set of packets as defined by interface component.

A virtual sensor can monitor multiple segments, and you can apply a different policy or configuration for each virtual sensor within a single physical sensor. You can set up a different policy per monitored segment under analysis. You can also apply the same policy instance, for example, sig0, rules0, or ad0, to different virtual sensors.

You can assign interfaces, inline interface pairs, inline VLAN pairs, and VLAN groups to a virtual sensor.

**Note**

The default virtual sensor is vs0. You cannot delete the default virtual sensor. The interface list, the anomaly detection operational mode, the inline TCP session tracking mode, and the virtual sensor description are the only configuration features you can change for the default virtual sensor. You cannot change the signature definition, event action rules, or anomaly detection policies.

Advantages and Restrictions of Virtualization

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 of 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.

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.

The following sensors support virtualization:

- IDS 4235
- IDS 4250
- IPS 4240
- IPS 4255
- IPS 4260

- IPS 4270-20
- AIP SSM

IDSM2 supports virtualization with the exception of VLAN groups on inline interface pairs.



Note AIM IPS, IDS 4215, and NM CIDS do not support virtualization.

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 and/or VLANs (or the subinterface for VLAN pairs).

The following options 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.

For More Information

- For more information on the modify packet inline event action, see [Event Actions, page 6-7](#).
- For more information on the Normalizer engine, see [Normalizer Engine, page A-19](#).

Configuring the Virtual Sensor

This section describes how to configure a virtual sensor, and contains the following topics:

- [Virtual Sensors Pane, page 4-4](#)
- [Virtual Sensor Pane Field Definitions, page 4-4](#)
- [Add and Edit Virtual Sensor Dialog Boxes Field Definitions, page 4-5](#)
- [Adding, Editing, and Deleting Virtual Sensors, page 4-5](#)

Virtual Sensors Pane

**Note**

You must be administrator or operator to configure a virtual sensor.

The Virtual Sensors pane displays a list of the virtual sensors. For each virtual sensor the following is displayed:

- Assigned interfaces/pairs
- Signature definition policy
- Event action rules policy
- Anomaly detection policy
- Anomaly detection operational mode setting
- Inline TCP session tracking mode
- Description of the virtual sensor

You can create, edit, or delete virtual sensors.

**Note**

The default virtual sensor is vs0. You cannot delete the default virtual sensor.

Virtual Sensor Pane Field Definitions

The following fields are found on the Virtual Sensor pane:

- Name—The name of the virtual sensor.
The default virtual sensor is vs0.
- Assigned Interfaces (or Pairs)—The interfaces or interface pairs that belong to this virtual sensor.
- Sig Definition Policy—The name of the signature definition policy.
The default signature definition policy is sig0.
- Event Action Rules Policy—The name of the event action rules policy.
The default event action rules policy is rules0.
- Anomaly Detection Policy—The name of the anomaly detection policy.
The default anomaly detection policy is ad0.
- AD Operational Mode—The mode (Detect, Inactive, Learning Accept) that anomaly detection is operating in.
- Inline TCP Session Tracking Mode—The mode (interface and VLAN, VLAN only, or virtual sensor) that is used to segregate multiple views of the same stream if the same stream passes through the sensor more than once.
- Description—The description of the virtual sensor.

For More Information

For more information on inline TCP session modes, see [Inline TCP Session Tracking Mode](#), page 4-3.

Add and Edit Virtual Sensor Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Virtual Sensor dialog boxes:

- Virtual Sensor Name—The name of the virtual sensor.
- Signature Definition Policy—The name of the signature definition policy that you want to assign to this virtual sensor. The default is sig0.
- Event Action Rules Policy—The name of the event action rules policy that you want to assign to this virtual sensor. The default is rules0.
- Anomaly Detection Policy—The name of the anomaly detection policy that you want to assign to this virtual sensor. The default is ad0.
- AD Operational Mode—The mode that you want the anomaly detection policy to operate in for this virtual sensor. The default is Detect.
- 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.
 - 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.
- Description—The description of the virtual sensor.
- Available Interfaces—Lets you assign and remove the interfaces to the virtual sensor.
 - Name—The list of available interfaces or interface pairs that you can assign to the virtual sensor.
 - Details—Lists the mode (Inline or Promiscuous) of the interface and the interfaces of the inline pairs.
 - Assigned—Whether the interfaces or interface pairs have been assigned to the virtual sensor.

Adding, Editing, and Deleting Virtual Sensors

You can apply the same policy instance, for example, sig0, rules0, and ad0, to different virtual sensors. The Add Virtual Sensor dialog box displays only the interfaces that are available to be assigned to this virtual sensor. Interfaces that have already been assigned to other virtual sensors are not shown in this dialog box.



Note

You must assign all interfaces to a virtual sensor and enable them before they can monitor traffic

To add, edit, and delete virtual sensors, follow these steps:

- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Choose **Configuration > Analysis Engine > Virtual Sensors**.

The Virtual Sensors pane appears.

- Step 3** To add a virtual sensor, click **Add**.

The Add Virtual Sensor dialog box appears.

- Step 4** Enter a name for the virtual sensor in the Virtual Sensor Name field.

- Step 5** Choose a signature definition policy from the drop-down list.

Unless you want to use the default sig0, you must have already added a signature definition policy by choosing **Configuration > Policies > Signature Definitions > Add**.

- Step 6** Choose an event action rules policy from the drop-down list.

Unless you want to use the default rules0, you must have already added a signature definition policy by choosing **Configuration > Policies > Event Action Rules > Add**.

- Step 7** Choose an anomaly detection policy from the drop-down list.

Unless you want to use the default ad0, you must have already added a signature definition policy by choosing **Configuration > Policies > Anomaly Detections > Add**.

- Step 8** Choose the anomaly detection mode (Detect, Inactive, Learning Accept) from the drop-down list.

The default is detect.

- Step 9** Choose how the sensor tracks inline TCP sessions (by interface and VLAN, VLAN only, or virtual sensor).

The default is virtual sensor. This is almost always the best option to choose.

- Step 10** Add a description of this virtual sensor in the Description field.

- Step 11** Assign the interface to the virtual sensor by selecting it and clicking **Assign**.



Note

Only the available interfaces are listed in the Available Interfaces list. If other interfaces exist, but have already been assigned to a virtual sensor, they do not appear in this list.



Tip

To discard your changes and close the Add Virtual Sensor dialog box, click **Cancel**.

- Step 12** Click **OK**.

The virtual sensor appears in the list in the Virtual Sensors pane.

- Step 13** To edit a virtual sensor, select it in the list, and then click **Edit**.

The Edit Virtual Sensor dialog box appears.

- Step 14** Edit any of the fields that you want to.

- Step 15** Click **OK**.

The edited virtual sensor appears in the list in the Virtual Sensors pane.



Tip

To discard your changes and close the Edit Virtual Sensor dialog box, click **Cancel**.

- Step 16** To remove a virtual sensor, select it, and then click **Delete**.

The virtual sensor no longer appears in the Virtual Sensors pane.

**Tip**

To discard your changes, click **Reset**.

Step 17 Click **Apply** to apply your changes and save the revised configuration.

For More Information

- For information on how to configure virtual sensors for AIP SSM, refer to [Configuring AIP SSM](#).
- For the procedure for enabling sensor interfaces, see [Enabling and Disabling Interfaces, page 3-17](#).
- For more information on configuring signature definitions policies, see [Configuring Signature Definition Policies, page 5-1](#).
- For more information on configuring event action rules policies, see [Configuring Event Action Rules Policies, page 6-11](#).
- For more information on configuring Anomaly Detection policies, see [Configuring Anomaly Detection Policies, page 7-8](#).
- For more information on Anomaly Detection modes, see [Anomaly Detection Modes, page 7-3](#).
- For more information on inline TCP session modes, see [Inline TCP Session Tracking Mode, page 4-3](#).

Configuring Global Variables

This section describes how to configure global variables, and contains the following topics:

- [Global Variables Pane, page 4-7](#)
- [Global Variables Pane Field Definitions, page 4-7](#)

Global Variables Pane

**Note**

You must be administrator or operator to configure global variables.

You can configure global variables inside the Analysis Engine component. There is only one global variable: Maximum Open IP Log Files.

Global Variables Pane Field Definitions

The following field is found in the Global Variables pane:

- Maximum Open IP Log Files—Maximum number of concurrently open IP log files.
The valid range is from 20 to 100. The default is 20.

