



CHAPTER 4

Analysis Engine

This chapter explains the function of Analysis Engine and how to assign interfaces to the virtual sensor. It contains the following sections:

- [Understanding Analysis Engine, page 4-1](#)
- [Configuring the Virtual Sensor, page 4-1](#)
- [Configuring Global Variables, page 4-4](#)

Understanding Analysis Engine

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

Configuring the Virtual Sensor

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

- [Overview, page 4-1](#)
- [Supported User Role, page 4-2](#)
- [Field Definitions, page 4-2](#)
- [Assigning Interfaces to the Virtual Sensor, page 4-3](#)

Overview

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 and from behind the firewall. IPS 5.1 only supports one virtual sensor, so a single sensor policy and configuration are applied to all monitored data streams.

Be aware of the following limitation when adding interfaces to the sensor—the same traffic flow cannot traverse the sensor twice either through the same interface in inline mode or through separate monitored interfaces. If packets from the same traffic flow traverse the sensor twice, the virtual sensor interprets the packets as duplicates, which results in false positive alerts.

You can configure NAT to change the IP address to handle this limitation. NAT causes the sensor to treat the before and after translation packets as separate flows. For example, if a firewall is using NAT from its internal to external networks, the sensor can monitor both of these networks without problem.

You can assign interfaces, interface pairs, and VLAN pairs to the virtual sensor and you can change the description of the virtual sensor, but you cannot add a virtual sensor or change the virtual sensor name.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the virtual sensor.

Field Definitions

This section lists the field definitions for the virtual sensor, and contains the following topics:

- [Virtual Sensor Pane, page 4-2](#)
- [Edit Virtual Sensor Dialog Box, page 4-2](#)

Virtual Sensor Pane

The following fields and buttons are found on the Virtual Sensor pane.

Field Descriptions:

- Name—The Name of the virtual sensor.
There is only one virtual sensor in IPS 5.1 and it is named vs0.
- Assigned Interfaces (or Pairs)—The interfaces or interface pairs that belong to this virtual sensor.
- Description—The description of the virtual sensor.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Edit Virtual Sensor Dialog Box

The following fields and buttons are found in the Edit Virtual Sensor dialog box.

Field Descriptions:

- Virtual Sensor Name—The name of the virtual sensor.
There is only one virtual sensor in IPS 5.1 and it is named vs0.
- Description—The description of the virtual sensor.

- **Assign Interfaces**—Lets you assign 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.

Button Functions:

- **Select All**—Lets you select all of the interfaces in the list.
- **Assign**—Adds the selected interface or interface pair to the Assigned Interfaces (or Pairs) list.
- **Remove**—Removes the selected interface or interface pair from the Assigned Interfaces (or Pairs) list.

Assigning Interfaces to the Virtual Sensor

To assign or remove an interface, inline interface pair, or inline VLAN pair from the virtual sensor, follow these steps:



Note

You must assign all interfaces to the virtual sensor and enable them before they can monitor traffic. For the procedures for enabling sensor interfaces, see [Chapter 3, “Configuring Interfaces.”](#)

-
- Step 1** Log in to IDM using an account with administrator or operator privileges.
- Step 2** Click **Configuration > Analysis Engine > Virtual Sensor**.
The Virtual Sensor pane appears.
- Step 3** Click **Edit**.
The Edit Virtual Sensor dialog box appears.
- Step 4** To assign an interface, inline interface pair, or inline VLAN pair to the virtual sensor, select it in the Available Interfaces (or Pairs) list, and click **Add**.
- Step 5** To remove an interface, inline interface pair, or inline VLAN pair from the virtual sensor, select it from the Assigned Interfaces (or Pairs) list, and click **Remove**.
- Step 6** To change the description from “default virtual sensor,” enter a new description in the Description field.



Tip

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

- Step 7** Click **OK**.
The interface appears in the list on the Virtual Sensor pane.



Tip

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

- Step 8** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring Global Variables

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

- [Overview, page 4-4](#)
- [Supported User Role, page 4-4](#)
- [Field Definitions, page 4-4](#)

Overview

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

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure global variables.

Field Definitions

The following fields and buttons are found on the Global Variables pane.

Field Descriptions:

- 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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.