IPS 6.X and later: Virtual Sensors with IME Configuration Example

Document ID: 111431

Contents

Introduction
Prerequisites
Requirements
Components Used
Related Products
Conventions
Background Information
About Analysis Engine
About Virtual Sensors
Advantages and Restrictions of Virtualization
Advantages of Virtualization
Restrictions of Virtualization
Virtualization Requirements
Configure
Add Virtual Sensors
Add Virtual Sensor with IME
Edit Virtual Sensors
Edit Virtual Sensor with IME
Delete Virtual Sensors
Delete Virtual Sensor with IME
Troubleshoot
IPS Manager Express does not Launch
Related Information

Introduction

This document explains the function of Analysis Engine and how to create, edit, and delete virtual sensors on the Cisco Secure Intrusion Prevention System (IPS) with Cisco IPS Manager Express (IME). It also explains how to assign interfaces to a virtual sensor.

Note: AIM−IPS and NME−IPS do not support virtualization.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4200 Series IPS Device that runs software version 6.0 and later
- Cisco IPS Manager Express (IME) version 6.1.1 and later

Note: While IME can be used to monitor sensor devices that run Cisco IPS 5.0 and later, some of the new features and functionality delivered in IME are only supported on sensors that run Cisco IPS 6.1 or later.

Note: Cisco Secure Intrusion Prevention System (IPS) 5.x supports only the default virtual sensor vs0. Virtual sensors other than the default vs0 are supported in IPS 6.x and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with these sensors:

- IPS−4240
- IPS−4255
- IPS−4260
- IPS−4270−20
- AIP−SSM

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

About 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. In order 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 based on the inline bypass configuration.

About Virtual Sensors

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: Cisco Secure Intrusion Prevention System (IPS) does not support more than four virtual sensors. 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

Advantages of Virtualization

Virtualization has these 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.

Restrictions of Virtualization

Virtualization has these restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- The use of VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
    - ♦ When you use 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 you use the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.

Virtualization Requirements

Virtualization has these 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.

Configure

In this section, you are presented with the information to add, edit, and delete virtual sensors.

Add Virtual Sensors

Issue the **virtual−sensor name** command in service analysis engine submode in order to create a virtual sensor. You assign policies (anomaly detection, event action rules, and signature definition) to the virtual sensor. Then you assign interfaces (promiscuous, inline interface pairs, inline VLAN pairs, and VLAN groups) to the virtual sensor. You must configure the inline interface pairs and VLAN pairs before you can assign them to a virtual sensor. These options apply:

- **anomaly−detection** Anomaly detection parameters.

- **anomaly−detection−name** name Name of the anomaly detection policy
- **operational−mode** Anomaly detection mode (**inactive, learn, detect**)

- **description** Description of the virtual sensor
- **event−action−rules** Name of the event action rules policy
- **inline−TCP−evasion−protection−mode** Lets you choose which type of Normalizer mode you need for traffic inspection:

  - **asymmetric** Can only see one direction of bidirectional traffic flow. Asymmetric mode protection relaxes the evasion protection at the TCP layer.

    Note: 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.
  - **strict** 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.

    Note: 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.
- **inline−TCP−session−tracking−mode** Advanced method that allows you to identify duplicate TCP session in inline traffic. The default is virtual sensor, which is almost always the best choice.

  - **virtual−sensor** All packets with the same session key (AaBb) within a virtual sensor belong to the same session.
  - **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 or interfaces are tracked independently.
  - **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 independently.
- **signature−definition** Name of the signature definition policy
- **logical−interfaces** Name of the logical interfaces (inline interface pairs)
- **physical−interfaces** Name of the physical interfaces (promiscuous, inline VLAN pairs, and VLAN groups)

  - **subinterface−number** The physical subinterface number. If the subinterface−type is none, the value of 0 indicates the entire interface is assigned in promiscuous mode.
  - **no** Removes an entry or selection

In order to add a virtual sensor, complete these steps:

1. Log in to the CLI with an account with administrator privileges.
2. Enter service analysis mode.

```
sensor# configure terminal

        sensor(config)# service analysis−engine

        sensor(config−ana)#
```

3. Add a virtual sensor.

```
sensor(config−ana)# virtual−sensor vs2

        sensor(config−ana−vir)#
```

4. Add a description for this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor 2
```

5. Assign an anomaly detection policy and operational mode to this virtual sensor.

```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad1

        sensor(config-ana-vir-ano)# operational-mode learn
```

6. Assign an event action rules policy to this virtual sensor.

```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules1
```

7. Assign a signature definition policy to this virtual sensor.

```
sensor(config-ana-vir)# signature-definition sig1
```

8. Assign the inline TCP session tracking mode.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```

The default is virtual sensor mode, which is almost always the best option to choose.

9. Assign the inline TCP evasion protection mode.

```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

The default is strict mode, which is almost always the best option to choose.

10. Display the list of available interfaces.

```
sensor(config-ana-vir)# physical-interface ?

        GigabitEthernet0/0     GigabitEthernet0/0 physical interface.

        GigabitEthernet0/1     GigabitEthernet0/1 physical interface.

        GigabitEthernet2/0     GigabitEthernet0/2 physical interface.

        GigabitEthernet2/1     GigabitEthernet0/3 physical interface.

        sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?

        <none available>
```

11. Assign the promiscuous mode interfaces you want to add to this virtual sensor.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

Repeat this step for all the promiscuous interfaces that you want to assign to this virtual sensor.

12. Assign the inline interface pairs you want to add to this virtual sensor.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

You must have already paired the interfaces.

13. Assign the subinterfaces of the inline VLAN pairs or groups you want to add to this virtual sensor as shown below:

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

You must have already subdivided any interfaces into VLAN pairs or groups.

14. Verify the virtual sensor settings.

```
sensor(config-ana-vir)# show settings
   name: vs2
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: GigabitEthernet0/2
         subinterface-number: 0 <defaulted>
      -----------------------------------------------
      inline-TCP-session-tracking-mode: virtual-sensor default: virtual-sensor
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

15. Exit analysis engine mode.

```
sensor(config-ana-vir)# exit
        sensor(config-ana)# exit
        sensor(config)#
        Apply Changes:?[yes]:
```

16. Press **Enter** in order to apply the changes or enter **no** to discard them.

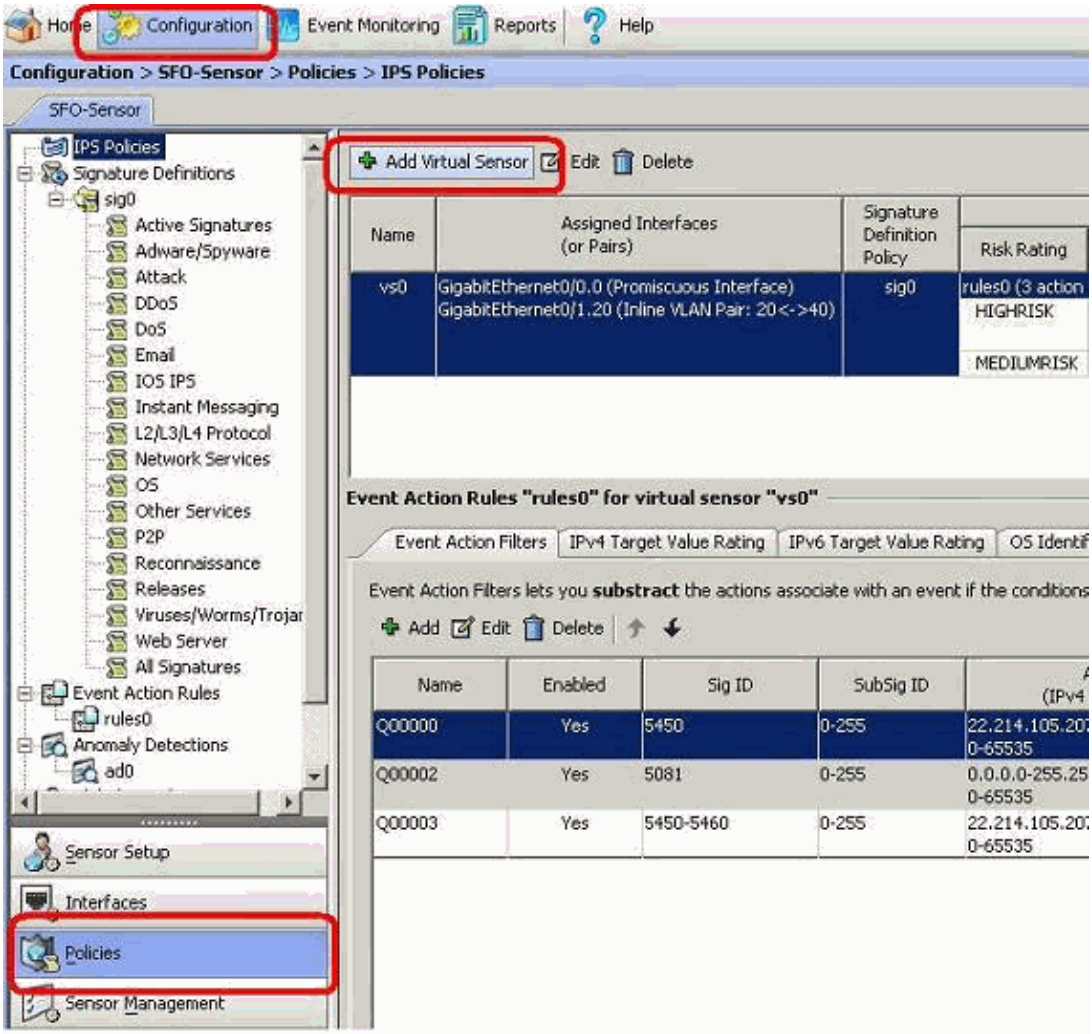
This completes the process to add a Virtual sensor to the Cisco Secure Intrusion Prevention System (IPS). Complete the same procedure to add more virtual sensors.

Note: Cisco Secure Intrusion Prevention System (IPS) does not support more than four virtual sensors. The default virtual sensor is vs0.

Add Virtual Sensor with IME

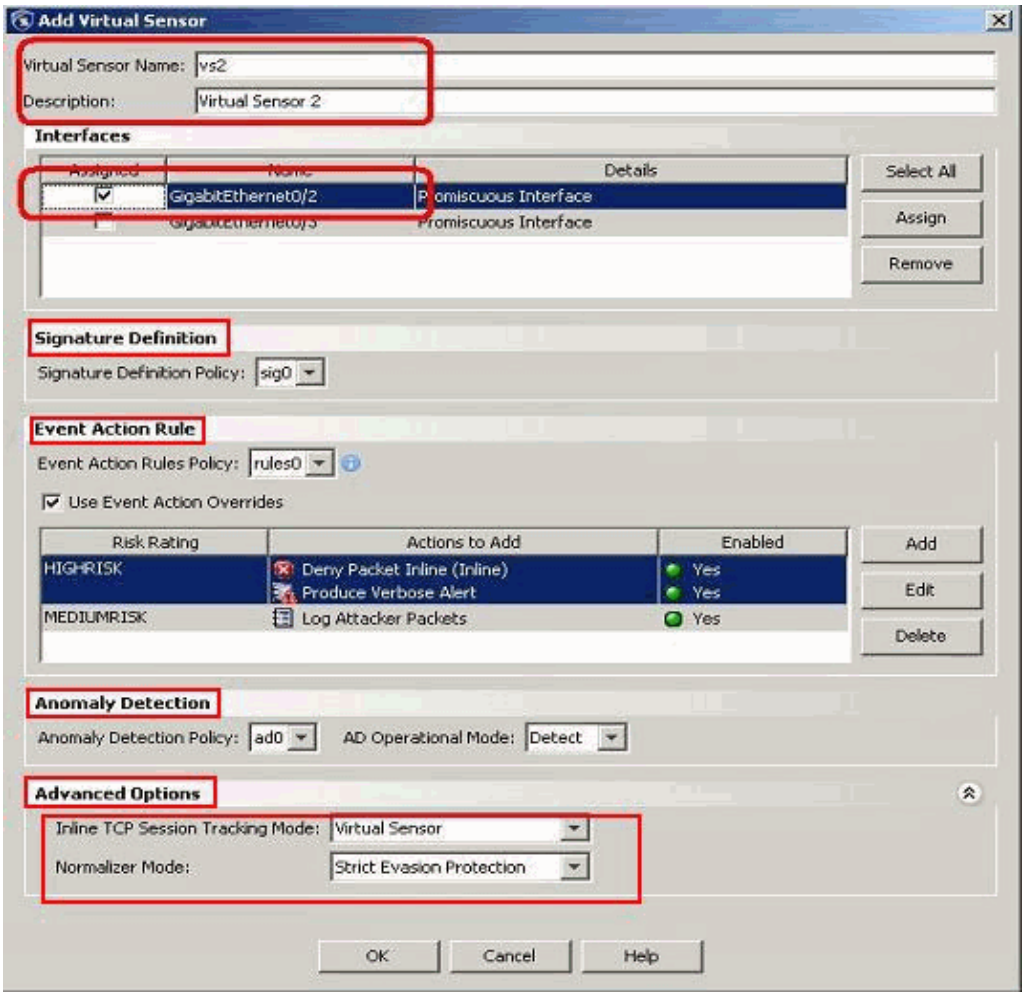
Complete these steps in order to configure a virtual sensor on Cisco Secure Intrusion Prevention System (IPS) with Cisco IPS Manager Express:

1. Choose **Configuration > SFO−Sensor> Policies> IPS Policies**. Then, click on **Add virtual sensor** as shown in the screenshot.

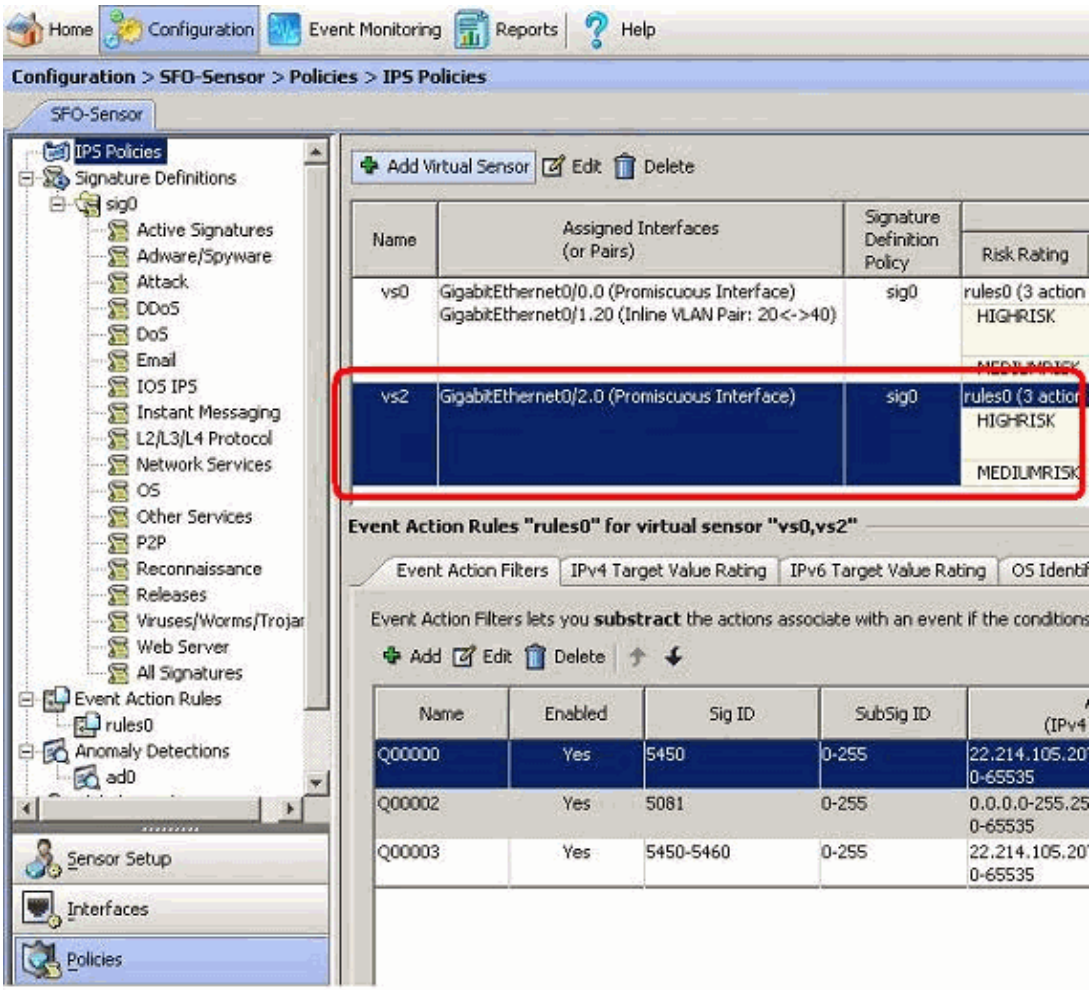


2. Name the virtual sensor (vs2 in this example) and add a description to the virtual sensor in the space provided. Also assign the promiscuous mode interfaces you want to add to this virtual sensor. Gigabit Ethernet 0/2 is chosen here. Now provide the details in the **signature definition**, **Event Action Rule**, **Anomaly Detection** and **Advanced options** sections as shown in the screen shot.

   Under **Advanced Options** provide the details about the TCP Session Tracking Mode and the Normalizer Mode. Here the **TCP Session Tracking Mode** is **virtual sensor** and the **Normalizer mode** is **Strict Evasion Protection** mode.



3. Click **OK**.
4. The newly added virtual sensor vs2 is shown in the list of virtual sensors. Click **Apply** for the new virtual sensor configuration to be sent to the Cisco Secure Intrusion Prevention System (IPS).



This completes the configuration to add a virtual sensor.

Edit Virtual Sensors

These parameters of a virtual sensor can be edited:

- Signature definition policy
- Event action rules policy
- Anomaly detection policy
- Anomaly detection operational mode
- Inline TCP session tracking mode
- Description
- Interfaces assigned

In order to edit a virtual sensor, complete these steps:

1. Log in to the CLI with an account with administrator privileges.
2. Enter service analysis mode.

```
sensor# configure terminal

        sensor(config)# service analysis-engine

        sensor(config-ana)#
```

3. Edit the virtual sensor, vs1.

```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#
```

4. Edit the description of this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor A
```

5. Change the anomaly detection policy and operational mode assigned to this virtual sensor.

```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad0

        sensor(config-ana-vir-ano)# operational-mode learn
```

6. Change the event action rules policy assigned to this virtual sensor.

```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules0
```

7. Change the signature definition policy assigned to this virtual sensor.

```
sensor(config-ana-vir)# signature-definition sig0
```

8. Change the inline TCP session tracking mode.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

   The default is virtual sensor mode, which is almost always the best option to choose.

9. Display the list of available interfaces.

```
sensor(config-ana-vir)# physical-interface ?

        GigabitEthernet0/0     GigabitEthernet0/0 physical interface.

        GigabitEthernet0/1     GigabitEthernet0/1 physical interface.

        GigabitEthernet2/0     GigabitEthernet0/2 physical interface.

        GigabitEthernet2/1     GigabitEthernet0/3 physical interface.

        sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?

        <none available>
```

10. Change the promiscuous mode interfaces assigned to this virtual sensor.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

11. Change the inline interface pairs assigned to this virtual sensor.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

    You must have already paired the interfaces.

12. Change the subinterface with the inline VLAN pairs or groups assigned to this virtual sensor.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

    You must have already subdivided any interfaces into VLAN pairs or groups.

13. Verify the edited virtual sensor settings.

```
sensor(config-ana-vir)# show settings
```

```
   name: vs2
   ------------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      ------------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      ------------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      ------------------------------------------------
         name: GigabitEthernet0/2
         subinterface-number: 0 <defaulted>
      ------------------------------------------------
      inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor
      ------------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
sensor(config-ana-vir)#
```

14. Exit analysis engine mode.

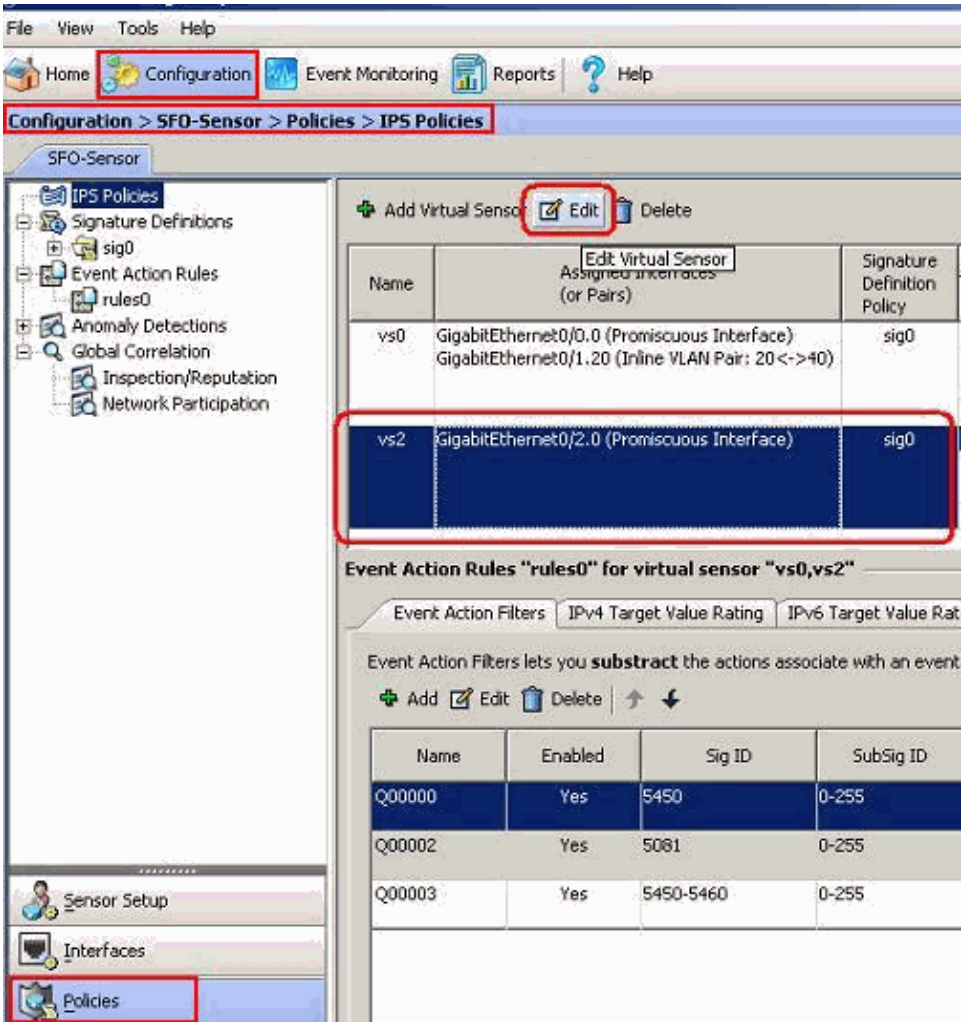
```
sensor(config-ana)# exit
        sensor(config)#
        Apply Changes:?[yes]:
```

15. Press **Enter** in order to apply the changes or enter **no** to discard them.

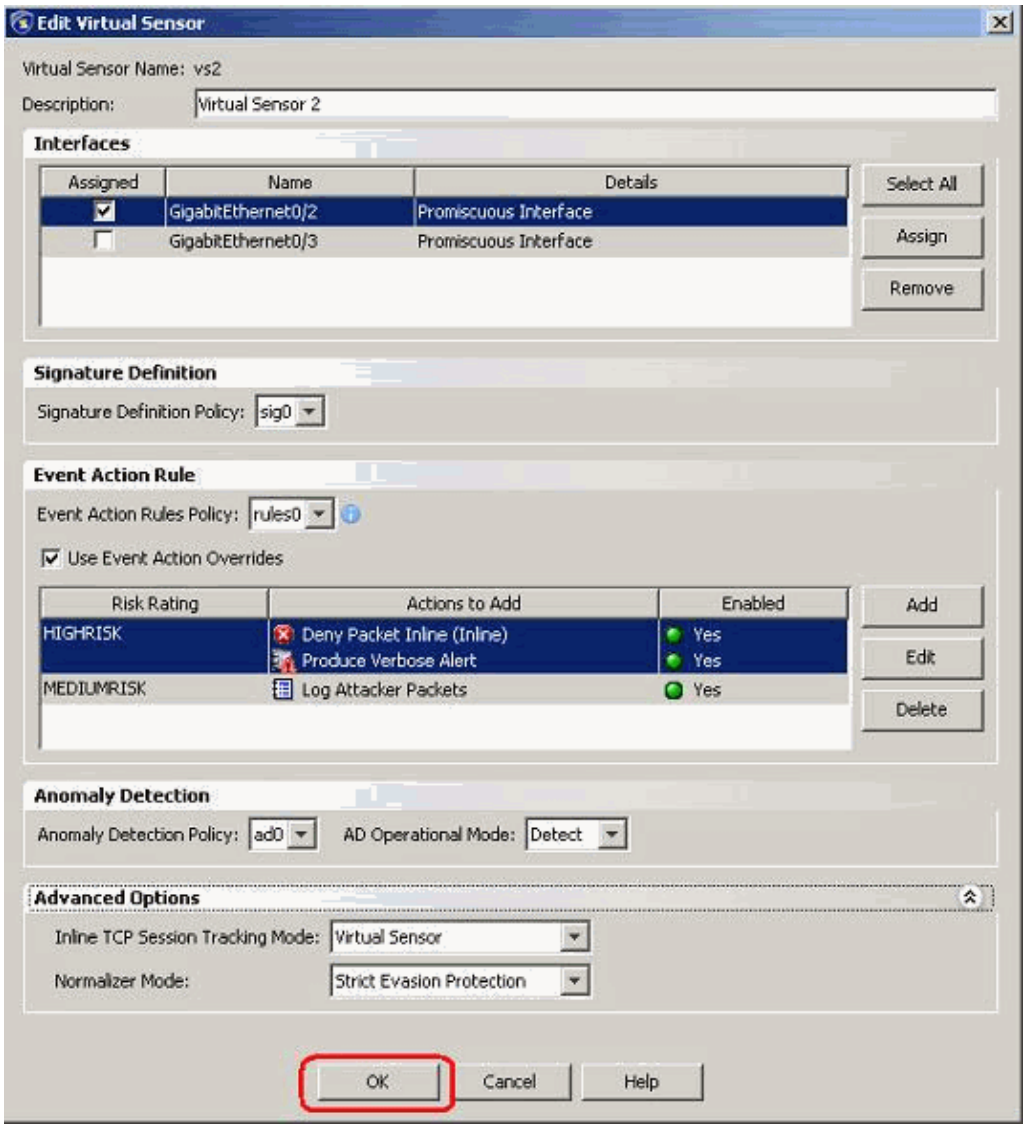
Edit Virtual Sensor with IME

Complete these steps in order to edit a virtual sensor on Cisco Secure Intrusion Prevention System (IPS) with Cisco IPS Manager Express:

1. Choose **Configuration > SFO-Sensor> Policies> IPS Policies**.
2. Choose the virtual sensor to be edited, and then click **Edit** as shown in the screenshot. In this example vs2 is the virtual sensor to be edited.



3. In the **Edit virtual sensor** window, make changes to the parameters for the virtual sensor present under the sections **signature definition**, **Event Action Rule**, **Anomaly Detection** and **Advanced options**. Click **OK**, and then click **Apply**.



This completes the process to edit a virtual sensor.

Delete Virtual Sensors

In order to delete a virtual sensor, complete these steps:

1. In order to delete a virtual sensor, issue the **no virtual−sensor** command.

```
sensor(config−ana)# virtual−sensor vs2

        sensor(config−ana−vir)#

        sensor(config−ana−vir)# exit

        sensor(config−ana)# no virtual−sensor vs2
```

2. Verify the deleted virtual sensor.

```
sensor(config−ana)# show settings

   global−parameters

   −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−

      ip−logging
```

```
      ----------------------------------------------

         max-open-iplog-files: 20 <defaulted>

      ----------------------------------------------

   ----------------------------------------------

   virtual-sensor (min: 1, max: 255, current: 2)

   ----------------------------------------------

      <protected entry>

      name: vs0 <defaulted>

      ----------------------------------------------

         description: default virtual sensor <defaulted>

         signature-definition: sig0 <protected>

         event-action-rules: rules0 <protected>

         anomaly-detection

         ----------------------------------------------

            anomaly-detection-name: ad0 <protected>

            operational-mode: detect <defaulted>

         ----------------------------------------------

         physical-interface (min: 0, max: 999999999, current: 0)

         ----------------------------------------------

         ----------------------------------------------

         logical-interface (min: 0, max: 999999999, current: 0)

         ----------------------------------------------

         ----------------------------------------------

sensor(config-ana)#
```

Only the default virtual sensor, **vs0**, is present.

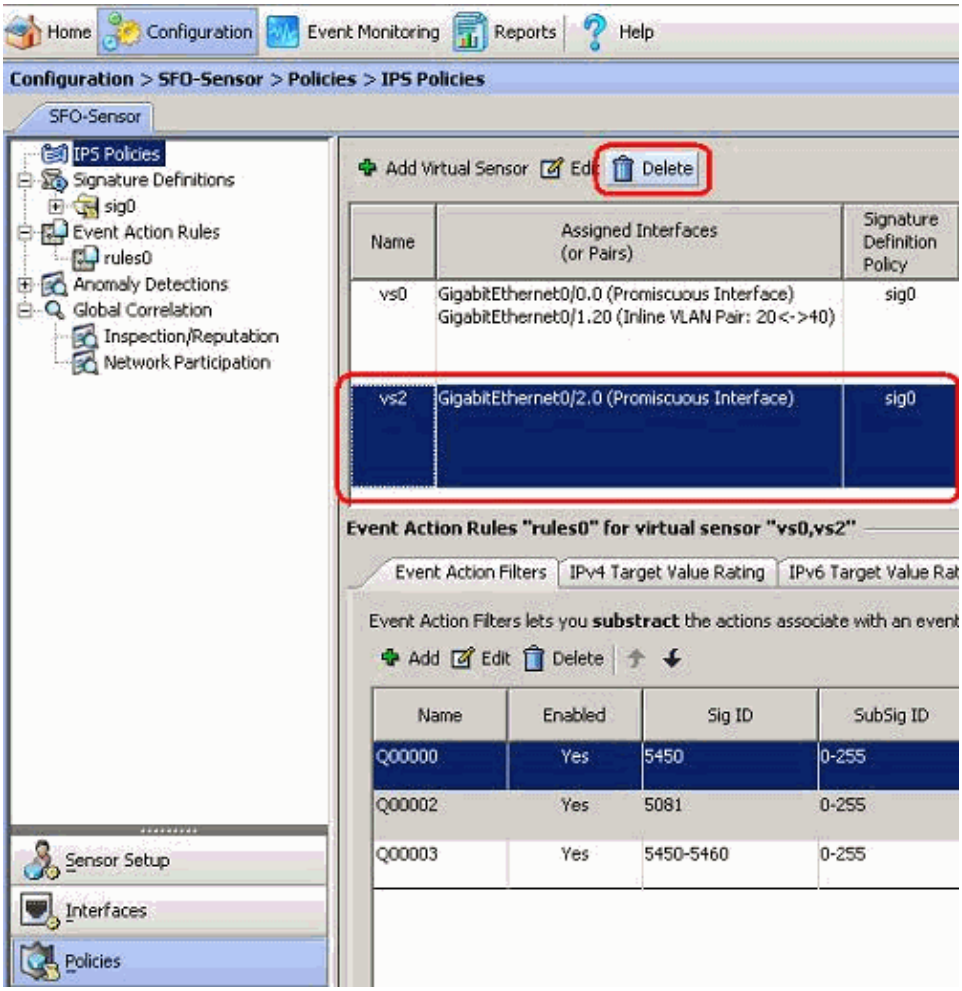
3. Exit analysis engine mode.

```
sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

Delete Virtual Sensor with IME

Complete this steps in order to delete a virtual sensor on Cisco Secure Intrusion Prevention System (IPS) with Cisco IPS Manager Express:

1. Choose **Configuration > SFO−Sensor> Policies> IPS Policies**.
2. Choose the virtual sensor to be deleted, and then click **Delete**, as shown in the screenshot. In this example vs2 is the virtual sensor to be deleted.



This completes the process to delete a virtual sensor. The virtual sensor vs2 is deleted.

Troubleshoot

IPS Manager Express does not Launch

Problem

When an attempt is made to access the IPS through the IME, IPS Manager Express does not start and this error message is received:

```
"Cannot start IME client. Please check if it is already started.
Exception: Address already in use: Cannot bind"
```

Solution

In order to resolve this, reload the IME workstation PC.

Related Information

- **Cisco Intrusion Prevention System Support Page**
- **Cisco IPS Manager Express Support Page**
- **Network Time Protocol (NTP)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 22, 2009 Document ID: 111431