CHAPTER 6

Configuring Virtual Sensors

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

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 Cisco IPS 6.1 does not support more than four virtual sensors. You cannot delete the default virtual sensor vs0.

Understanding 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 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:

- IPS 4240
- IPS 4255
- IPS 4260

- IPS 4270-20
- AIP SSM

IDSM2 supports virtualization with the exception of VLAN groups on inline interface pairs. The AIM IPS and NME IPS 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 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.

For More Information

- For more information on the modify packet inline event action, see Event Actions, page 7-8.
- For more information on the Normalizer engine, see Normalizer Engine, page B-22.

Adding, Editing, and Deleting Virtual Sensors

This section describes how to add, edit, and delete virtual sensors, and contains the following topics:

Adding Virtual Sensors

Note You can create four virtual sensors.

Use the **virtual-sensor** *name* command in service analysis engine submode 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.

The following options apply:

- **anomaly-detection**—Anomaly detection parameters.
  - **anomaly-detection-name** *name*—Name of the anomaly detection policy.
  - **operational-mode {inactive**, **learn**, **detect}**—Anomaly detection modes.
- **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 by which 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.

To add a virtual sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter service analysis mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Add a virtual sensor.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Add a description for this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor 1
```

Step 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
```

Step 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
```

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

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

Step 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.

Step 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.

Step 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>
```

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

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/3
```

Repeat Step 11 for all the promiscuous interfaces that you want to assign to this virtual sensor.

Step 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.

Step 13 Assign the subinterfaces of the inline VLAN pairs or groups you want to add 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.

Step 14 Verify the virtual sensor settings.

```
sensor(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      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: GigabitEthernet0/3
         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)#
```

Step 15 Exit analysis engine mode.

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

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

For More Information

- For the procedure for creating virtual sensors on the AIP SSM, see Creating Virtual Sensors, page 18-3.
- For more information on creating and configuring anomaly detection policies, see Working With Anomaly Detection Policies, page 9-8.

- For more information on creating and configuring event action rules policies, see Working With Event Action Rules Policies, page 7-11.
- For more information on creating and configuring signature definition policies, see Working With Signature Definition Policies, page 8-1.
- For the procedure for pairing inline interfaces, see Configuring Inline Interface Pairs, page 5-16. Repeat Step 11 for all the inline interface pairs that you want to assign to this virtual sensor.
- For the procedure for pairing and grouping inline VLANs, see Configuring Inline VLAN Pairs, page 5-21 and Configuring VLAN Groups, page 5-27. Repeat Step 12 for all inline VLAN pairs or VLAN groups that you want to assign to this virtual sensor.

Editing and Deleting Virtual Sensors

You can edit the following parameters of a virtual sensor:

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

To edit or delete a virtual sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter analysis engine mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Edit the virtual sensor, vs1.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Edit the description of this virtual sensor.

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

Step 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
```

Step 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
```

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

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

Step 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.

Step 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>
```

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

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

Step 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.

Step 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.

Step 13 Verify the edited virtual sensor settings.

```
ssensor(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      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: GigabitEthernet0/3
         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)#
```

Step 14 To delete a virtual sensor:

```
sensor(config-ana-vir)# exit
sensor(config-ana)# no virtual-sensor vs1
```

Step 15 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.

Step 16 Exit analysis engine mode.

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

Step 17 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For more information on creating and configuring anomaly detection policies, see Working With Anomaly Detection Policies, page 9-8.
- For more information on creating and configuring event action rules policies, see Working With Event Action Rules Policies, page 7-11.
- For more information on creating and configuring signature definition policies, see Working With Signature Definition Policies, page 8-1.
- For the procedure for pairing inline interfaces, see Configuring Inline Interface Pairs, page 5-16. Repeat Step 11 for all the inline interface pairs that you want to assign to this virtual sensor.
- For the procedure for pairing and grouping inline VLANs, see Configuring Inline VLAN Pairs, page 5-21 and Configuring VLAN Groups, page 5-27. Repeat Step 12 for all inline VLAN pairs or VLAN groups that you want to assign to this virtual sensor.

Configuring Global Variables

Note Configuring the maximum number of open IP log files is the only global variable in Cisco IPS 6.1.

Use the **global-parameters** command in service analysis engine submode to create global variables.

The following options apply:

- **ip-logging**—Global IP logging parameters.
  - **max-open-iplog-files**—The maximum number of concurrently open log files. The range is 20 to 100. The default is 20.

To create a global variable, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter service analysis mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Create the variable for the maximum number of open IP logs.

```
sensor(config-ana)# global-parameters
sensor(config-ana-glo)# ip-logging
sensor(config-ana-glo-ip)# max-open-iplog-files 50
```

Step 4 Verify the global variable settings:

```
sensor(config-ana-glo-ip)# show settings
   ip-logging
   -----------------------------------------------
      max-open-iplog-files: 50 default: 20
   -----------------------------------------------
sensor(config-ana-glo-ip)#
```

Step 5 Exit analysis engine mode.

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

Step 6 Press **Enter** to apply the changes or enter **no** to discard them.