



CHAPTER 18

Managing IPS Devices

Network sensing in support of intrusion prevention can be accomplished using a sensor, an IDSM (Intrusion Detection System Module), a Cisco IOS router running IOS IPS, and line-card modules running in certain Cisco IOS routers. These sensing platforms are components of the Cisco Intrusion Prevention System and can be managed by Cisco Security Manager.

These sensing platforms monitor and analyze network traffic in real time. They do this by looking for anomalies and misuse on the basis of an extensive embedded signature library. However, these platforms differ in how they can respond to perceived intrusions.

The following topics describe how to manage IPS devices (Cisco IPS sensors and Cisco IOS IPS devices):

- [Identifying Allowed Hosts, page 18-2](#)
- [Configuring SNMP, page 18-2](#)
- [Configuring the External Product Interface, page 18-5](#)
- [Identifying an NTP Server, page 18-9](#)
- [Configuring Logging, page 18-10](#)
- [Configuring Blocking, page 18-11](#)
- [Configuring Virtual Sensors, page 18-12](#)

Identifying Allowed Hosts

By default, all hosts on your network can connect to a sensor to configure it and receive alarm data from it. However, you can identify the hosts that are allowed to connect to a sensor, and no other hosts will be allowed to connect.

This procedure describes how to identify allowed hosts for a sensor.

**Note**

If you do not identify the Security Manager server as an allowed host, then you will not be able to connect to your sensors or manage them.

-
- Step 1** In Device View, select the sensor for which you want to add an allowed host.
 - Step 2** Also in Device View, select **Platform > Device Admin > Device Access > Allowed Hosts**. The Allowed Hosts summary page appears.
 - Step 3** Click the **Add** button. The Add Access List dialog box appears.
 - Step 4** Enter the network address of the allowed host you want to add, or click the **Select** button and select the allowed host in the Networks/Hosts Selector dialog box that appears. Allowed hosts should be entered in prefix notation: <IP network> / subnet mask. For example, 64.0.0.0/8. The hosts available via Select button can be predefined from the Security Manager Policy Object Manager (Tools > Policy Object Manager > Networks/Hosts).
 - Step 5** Click OK. The Allowed Hosts summary page appears, updated to show the host that you just added.
 - Step 6** Click **Save** to apply your changes and save the revised configuration.
-

Configuring SNMP

SNMP is a simple request/response application-layer protocol for the exchange of management information between network devices. In SNMP, there are a network-management system, which issues a request, and managed devices, which return responses. SNMP implements these requests and responses by using

one of four protocol operations: Get, GetNext, Set, and Trap. An SNMP trap is a notification. You can configure an IPS sensor to send a trap to classify an event as a warning, as an error, or as fatal.

The General Configuration tab on the SNMP page enables you to configure certain general SNMP parameters:

- **Enable SNMP Gets/Sets**—Allows you to enable the sensor to respond to get and set queries. If this field is disabled, the sensor does not respond to the query.
- **Read-Only Community String**—Sets the read-only community string of the sensor to a string you specify. When a sensor receives an SNMP get request with the specified read-only community string, it responds. This string gives access to all SNMP get requests.
- **Read-Write Community**—Sets the read-write community string of the sensor to a string you specify. When a sensor receives an SNMP get request, or an SNMP set request, with the specified read-write community string, it responds. This string gives access to all SNMP get requests and set requests.
- **Sensor Agent Port**—Instructs a sensor to run SNMP Agent in the specified port. Valid port numbers range from 1 to 65535.
- **Protocol**—Instructs a sensor to run SNMP on top of particular transport protocol. The options available are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

The SNMP Trap Configuration tab on the SNMP page enables you to configure SNMP traps, to enable error events notification, to enable detailed traps, and to modify the default trap community string:

- **Enable Traps**—Allows you to enable the sensor to notify interested parties whenever a specific type of event occurs in a sensor. When you select this check box, the sensor is instructed to perform notification. (You can also use the Traps Destination function to configure interested parties.) If the Enable Traps check box is not selected, the sensor does not respond to the query.
- **Select the error events to notify through SNMP**—Use this set of check boxes to specify the level of notifications that are enabled. The three levels of notification are Fatal, Error, and Warning. When you select one or more of these check boxes, you enable the sensor to send notification of events that correspond to the levels selected.
- **Enable detailed traps for alerts**—When you select this check box, you enable the sensor to send the detailed traps for all alerts.

- **Default Trap Community String**—All traps that are being notified carry a community string. All traps that have a community string identical to that of the destination are taken by the destination. All other traps are discarded by the destination. This is a primary default condition, but this default can also be overridden at any destination.

This procedure describes how to configure general SNMP parameters and how to configure SNMP traps.

-
- Step 1** In Device view, select the sensor for which you want to configure general SNMP parameters or SNMP traps or both.
- Step 2** Also in Device View, select **Platform > Device Admin > Device Access > SNMP**. The SNMP summary page appears, and the General Configuration tab is visible by default. The General Configuration tab displays the general SNMP parameters, which are the parameters that the SNMP management workstation (on the Security Manager server) can request from the SNMP agent (on the sensor).
- Step 3** Check the **Enable SNMP Gets/Sets** check box to enable the sensor to respond to get and set queries.
- Step 4** In the Read-Only Community String field, enter the read-only community string. The read-only community string helps identify the SNMP agent (on the sensor).
- Step 5** In the Read-Write Community String field, enter the read-write community string. The read-write community string helps identify the SNMP agent (on the sensor).



Note The management workstation (on the Security Manager server) sends SNMP requests to the SNMP agent (on the sensor). If the management workstation issues a request and the community string does not match what is on the sensor, the sensor rejects it.

- Step 6** In the Sensor Contact field, enter the user ID of the person who is the sensor contact.
- Step 7** In the Sensor Location field, enter the location of the sensor.
- Step 8** In the Sensor Agent Port field, enter the port of the SNMP agent (on the sensor). The default SNMP port number is 161.
- Step 9** From the Sensor Agent Protocol drop-down list, choose the protocol that the SNMP agent (on the sensor) will use. The default protocol is UDP.
- Step 10** Click **Save** to apply your changes and save the revised configuration.

- Step 11** Click the **SNMP Trap Configuration** tab. The SNMP trap configuration fields are visible on this tab.
 - Step 12** To enable SNMP traps, check the **Enable Notifications** check box.
 - Step 13** In the Error Filter area, select the type(s) of error events you want to be notified about through SNMP traps. The types of error events you can select are Warning, Error, and Fatal.
 - Step 14** To receive detailed SNMP traps, check the **Enable Detail Traps** check box.
 - Step 15** In the Default Trap Community String field, enter the community string to be included in the detailed traps.
 - Step 16** In the Trap Destinations area, click the **Add** button. The Add SNMP Trap Communication dialog box appears.
 - Step 17** In the IP Address field, enter the IP address of the SNMP management station (on the Security Manager server).
 - Step 18** In the Trap Community String field, enter the trap Community string.
 - Step 19** In the Trap Port field, enter the UDP port or the TCP port of the SNMP management station (on the Security Manager server), depending upon whether you chose UDP or TCP in the Sensor Agent Protocol drop-down list on the General Configuration tab.
 - Step 20** Click **Save** to apply your changes and save the revised configuration.
-

Configuring the External Product Interface

The External Product Interface tab in the Server Access folder enables you to configure Management Center for Cisco Security Agents settings.

In general, the external product interface is designed to receive and process information from external security and management products. These external security and management products collect information that can be used to automatically enhance the sensor configuration information. In particular, in IPS 6.0, Management Center for Cisco Security Agents is the only external product that can be configured to communicate with the IPS. At most two Management Center for Cisco Security Agents servers can be configured per IPS.

Management Center for Cisco Security Agents enforces a security policy on network hosts. It has two components:

- Agents that reside on and protect network hosts.
- A management console—An application that manages agents. It downloads security policy updates to agents and uploads operational information from agents.

For detailed information on Management Center for Cisco Security Agents, refer to [About CSA MC](#) in *Installing and Using Cisco Intrusion Prevention System Device Manager 6.0*. (You will be prompted to log in.)

Before You Begin

Add the external product as an allowed host so that Security Manager allows the sensor to communicate with the external product. For more information, refer to [Identifying Allowed Hosts](#), page 18-2.

This procedure describes how to add, edit, and delete external product interfaces and posture ACLs.

-
- Step 1** In Device View, select the sensor for which you want to configure an external product interface.
- Step 2** Also in Device View, select **Platform > Device Admin > Server Access > External Product Interface**. The External Product Interface page appears, and the Management Center for Cisco Security Agents tab is active.
- Step 3** Click the **Add** button. The Add External Product Interface dialog box appears.
- Step 4** In the External Product's IP Address field, enter the IP address of the external product.
- Step 5** In the Port field, change the default port 443 if you need to.
- Step 6** Configure the authentication settings:
- a. In the User name field, enter the user name of the user who can log in to the external product.
 - b. In the Password field, enter the password the user will use.
- Step 7** (Optional) Check the **Enable receipt of host postures** check box to allow the host posture information to be passed from the external product to the sensor. This check box is selected by default, so you must deselect it if you do not want this configuration.



Note If you do not check the **Enable receipt of host postures** check box, the host posture information received from the Management Center for Cisco Security Agents is deleted.

Step 8 (Optional) Check the **Allow unreachable hosts' postures** check box to allow the host posture information from unreachable hosts to be passed from the external product to the sensor. This check box is selected by default, so you must deselect it if you do not want this configuration.



Note A host is not reachable if the Management Center for Cisco Security Agents cannot establish a connection with the host on any of the IP addresses in the host's posture. This option is useful in filtering the postures whose IP addresses may not be visible to the IPS or may be duplicated across the network. This filter is most applicable in network topologies where hosts that are not reachable by the Management Center for Cisco Security Agents are also not reachable by the IPS, for example if the IPS and the Management Center for Cisco Security Agents are on the same network segment.

Step 9 (Optional) Configure the watch list settings:

- a. Check the **Enable receipt of watch listed addresses** check box to allow the watch list information to be passed from the external product to the sensor. This check box is selected by default, so you must deselect it if you do not want this configuration.



Note If you do not check the **Enable receipt of watch listed addresses** check box, the watch list information received from the Management Center for Cisco Security Agents is deleted.

- b. In the Manual Watch List RR (Risk Rating) increase field, you can change the percentage from the default of 25. The valid range is 0 to 35.
- c. In the Session-based Watch List RR Increase field, you can change the percentage from the default of 25. The valid range is 0 to 35.
- d. In the Packet-based Watch List RR Increase field, you can change the percentage from the default of 10. The valid range is 0 to 35.

- Step 10** (Optional) Click the **Add** button to add a posture ACL (Access Control List). The Add Posture ACL dialog box appears.



Note Posture ACLs are network address ranges for which host postures are allowed or denied. Use posture ACLs to filter postures that have IP addresses that may not be visible to the IPS or may be duplicated across the network.

- Step 11** (Optional unless you chose to add a posture ACL) In the Network Address field, enter the network address the posture ACL will use.
- Step 12** (Optional unless you chose to add a posture ACL) In the Action drop-down list, choose the action (Deny or Permit) the posture ACL will take.
- Step 13** (Optional unless you chose to add a posture ACL) Click **OK**.
The new posture ACL appears in the Posture ACLs list in the Add External Product Interface dialog box.
You can use the **Move Up** and **Move Down** buttons to reorder the posture ACLs that you create.
ACLs will be applied in order from the top of the list to the bottom.
- Step 14** To modify an existing posture ACL, select it, and then click the **Edit** button. The Modify Posture ACL dialog box appears.
- Step 15** Modify the Network Address and Action fields.
- Step 16** Click **OK**. The modified posture ACL appears in the Posture ACLs list in the Add External Product Interface dialog box.
- Step 17** To delete a posture ACL from the list, select it, and then click the **Delete** button.
The posture ACL no longer appears in the Posture ACLs list in the Add External Product Interface dialog box.
- Step 18** Click **OK**. The external product interface now appears in the Management Center for Cisco Security Agents settings summary table.
- Step 19** To edit the external product interface, select it, and then click the **Edit** button. The Edit External Product Interface dialog box appears.
- Step 20** Make any changes needed to the fields in the dialog box.
- Step 21** Click **OK**. The edited external product interface appears in the Management Center for Cisco Security Agents settings summary table.

- Step 22** To delete an external product interface, select it, and then click the **Delete** button. The external product interface no longer appears in the Management Center for Cisco Security Agents settings summary table.
- Step 23** Click **Save** to apply your changes and save the revised configuration.
-

Identifying an NTP Server

Network Time Protocol (NTP) server time can be used with a sensor if the sensor is managed by Security Manager.

For detailed information on how to set the time on a sensor, refer to [Configuring the Sensor to Use an NTP Time Source](#) in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface Version 6.0*.



Tip

Check the time on your IPS sensor if you are having trouble updating your IPS software. If the time on the sensor is ahead of the time on the associated certificate, the certificate is rejected, and the sensor software update fails.

- Step 1** In Device view, select the IPS sensor for which you want to identify an NTP server.
- Step 2** Select **Platform > Device Adman > Server Access > NTP**. The Network Time Protocol page appears.
- Step 3** In the NTP Server IP Address field, enter the address of the NTP server. You can use the Select button to select previously defined hosts from the Security Manager Policy Object Manager (Tools > Policy Object Manager > Networks/Hosts).
- Step 4** In the Key field, enter the key value of the NTP server. The key is an MD5 type of key (either numeric or character); it is the key that was used to set up the NTP server.
- Step 5** In the Key ID field, enter the key ID value of the NTP server.
- Step 6** Click **Save** to save your definitions to the Security Manager server.
-

Configuring Logging

The Logging page in the Platform folder in Device view is where you configure traffic flow notifications and Analysis Engine global variables.

Traffic flow notifications have to do with the flow of traffic across the interface of a sensor. You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts and stops) during a specified interval. You can configure the missed packet threshold within a specific notification interval and also configure the interface idle delay before a status event is reported.

This procedure describes how to configure traffic flow notifications.

-
- Step 1** In Device view, select an IPS sensor from the Device selector.
 - Step 2** Select **Platform > Logging**. The Logging page appears with the Interface Notifications tab selected.
 - Step 3** Determine the percent of missed packets that has to occur before you want to receive notification and enter that amount in the Missed Packets Threshold field.
 - Step 4** Determine the amount of seconds that you want to check for the percentage of missed packets and enter that amount in the Notification Interval field.
 - Step 5** Determine the amount of seconds that you will allow an interface to be idle and not receiving packets before you want to be notified and enter that in the Interface Idle Threshold field.
-

Configuring Analysis Engine Global Variables

The Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces. For the Analysis Engine, there is only one global variable: Maximum Open IP Log Files.

This procedure describes how to configure Analysis Engine global variables.

-
- Step 1** In Device view, select an IPS sensor from the Device selector.
 - Step 2** Select **Platform > Logging**. The Logging page appears.

- Step 3** Select the **Analysis Engine** tab.
- Step 4** Determine the maximum number of open IP log files that you want to have and enter that value in the Maximum Open IP Log Files field. The valid range is from 20 to 100. The default is 20.
-

Configuring Blocking

Blocking is one of the most common and well-established responses that is made by Cisco IPS when it detects an intrusion or malicious activity. In Cisco IPS, block means to block attacks on your network by blocking offending traffic: The IPS device communicates with a network device such as a Cisco IOS router and applies an access control list (ACL) entry specifying that the source address of the attack be denied.

To configure blocking in Security Manager, you must specify the network device that performs the blocking and then specify several parameters to configure blocking as an effective response that protects your network. A network device that performs blocking is called a blocking device. Before you can use a network device as a blocking device, you must identify it in Security Manager and specify its properties.

Many network devices can be used to support blocking: Cisco IOS routers, Cisco firewalls, and Catalyst 6000-series switches.

An essential part of configuring blocking is identify hosts and networks that should never be blocked. For example, you may have a trusted network device whose normal, expected behavior mimics an attack. But such a device should never be blocked. Also, trusted, internal networks should never be blocked, such as the network where Security Manager is running.



Note

In IOS IPS, you cannot identify hosts and networks that should never be blocked.

Attack Response Control (ARC) is responsible for rate limiting traffic in protected networks. Rate limiting lets sensors restrict the rate of specified traffic classes on network devices. Rate limit responses are supported for the Host Flood

and Net Flood engines, and the TCP half-open SYN signature. ARC can configure rate limits on network devices running Cisco IOS version 12.3 or later. Rate limiting can be configured with Security Manager on the Blocking page.

In some configurations it may be more effective to have a proxy sensor that controls blocking on one or more network devices on behalf of one or more other sensors.

These proxy sensors are referred to as master blocking sensors. Rate limit requests can be forwarded to other sensors using the master blocking sensor forwarding mechanism.

**Note**

Attack Response Control (ARC) was previously referred to as Network Access Control.

Use the Blocking page in the Security folder to specify the devices that will perform blocking and to specify other parameters.

Configuring Virtual Sensors

The Virtual Sensors page is where you create, name, and configure virtual sensors on your Cisco IPS devices. A virtual sensor is a logical grouping of sensing interfaces and the configuration policy for the signature engines and event action filters to apply.

The process of creating and naming virtual sensors on your Cisco IPS devices is sometimes called “virtualization.” Virtualization is the separation of a single physical IPS device into two or more logical devices on the basis of port, IP address range, VLAN tag, and other criteria.

**Note**

Not all Cisco IPS 4200 Series Sensors support virtual sensors; specifically, the Cisco IPS 4215 does not support virtual sensors. IDSM2 supports virtualization except for vlan-groups on inline-interface-pairs. NM-CIDS does not support virtualization.

**Note**

Not all versions of Cisco Intrusion Prevention System support virtual sensors; specifically, support for virtual sensors requires Cisco IPS 6.0 or later.

**Note**

Virtual sensors are not supported by Cisco IOS IPS.

Creating a virtual sensor involves signature policies, event action policies, anomaly detection policies, and interfaces. More specifically, creating a virtual sensor involves the following policy configuration instances:

- Signature definition (optional)
- Anomaly detection (optional)
- Anomaly detection operation mode (optional)
- Event action rules (optional)
- List of assigned/available interfaces (required)

After defining these policies, you need to apply these policies to the virtual sensor.

**Note**

The Virtual Sensors policy cannot be inherited or shared.

Advantages 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, Security Manager enables you to do so.

You can configure up to four virtual sensors on one appliance, but you can add only three (the number four being the sum of vs0, the default virtual sensor, and the three that you can add). No packet is processed by more than one virtual sensor.

In summary, 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 disadvantages:

- 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.

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; however, you can edit it and change the interfaces, anomaly detection mode, inline TCP session tracking mode, and the description.

Assigning Interfaces to Virtual Sensors

A Cisco IPS sensor monitors traffic that traverses (1) interfaces, (2) interface pairs, or (3) 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
- inline interface pair
- inline VLAN pair
- promiscuous VLAN group
- inline VLAN group

A promiscuous VLAN group is a VLAN group assigned to a subinterface on an interface. The 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.

An inline VLAN group is a VLAN group assigned to a subinterface of an existing 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.

Viewing Your Virtual Sensors

This procedure describes how to see a summary table of all the virtual sensors for a particular IPS device.

-
- Step 1** In Device view, select an IPS device from the Device selector.
 - Step 2** Select **Virtual Sensors**. The Main Virtual Sensor Table appears.
-

Defining A Virtual Sensor

This procedure describes how to define, or add, a virtual sensor for an IPS device.

-
- Step 1** In Device view, select an IPS device from the Device selector.
 - Step 2** Select **Virtual Sensors**. The Main Virtual Sensor Table appears.
 - Step 3** Click the **Add** button. The Add Virtual Sensor dialog box appears.
 - Step 4** Enter the Virtual Sensor Name, Anomaly Detection Mode, and Inline TCP Session Tracking Mode.
 - Step 5** Click **OK** to save your changes.



Note The display name of the real device is prepended to the beginning of the name of the virtual sensor. As a result, the virtual sensors appear next to the 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 6** Click **Save**.



Note After you click **Save**, you must click **File > Submit** for the new virtual sensor to appear in the device list. After you click **File > Submit**, a moment is required for the new virtual sensor to appear.

Editing A Virtual Sensor

This procedure describes how to edit a virtual sensor for an IPS device.

-
- Step 1** In Device view, select an IPS device from the Device selector.
 - Step 2** Select **Virtual Sensors**. The Main Virtual Sensor Table appears.
 - Step 3** Click the **Edit** button. The Edit Virtual Sensor dialog box appears.
 - Step 4** Edit the Virtual Sensor Name, Anomaly Detection Mode, and Inline TCP Session Tracking Mode.
 - Step 5** Click **OK** to save your changes.
-

Deleting A Virtual Sensor

This procedure describes how to delete a virtual sensor from an IPS device.

-
- Step 1** In Device view, select an IPS device from the Device selector.
 - Step 2** Select **Virtual Sensors**. The Main Virtual Sensor Table appears.
 - Step 3** Select a virtual sensor in the summary table.



Note You cannot delete vs0, the default virtual sensor.

- Step 4** Click the **Delete** button. The virtual sensor that you selected is deleted.

**Note**

After you delete a virtual sensor, it will take a few moments before the device view is updated and the virtual sensor disappears from the list of devices.
