



CHAPTER 13

Managing IPS Services

Cisco Security Manager supports the management and configuration of Cisco Intrusion Prevention System (IPS) sensors (appliances, switch modules, network modules, and Security Service modules [SSMs]) and Cisco IOS IPS devices (Cisco IOS routers with IPS-enabled images and Cisco Integrated Services Routers [ISRs]). You configure IPS sensors and IOS IPS devices through the use of policies, each of which defines a different part of the configuration of the sensor. For a detailed explanation of the policy paradigm used by Cisco Security Manager, see the “Managing Policies” chapter.

By right-clicking a policy type in one of the policy selectors, you can assign a policy to a single sensor or IOS IPS device, share the policy among more than one sensor or IOS IPS device, or unassign the policy from the sensor or IOS IPS device. For more information about the options available from this shortcut menu, see Policy Selector Shortcut Menu Options.

The following topics describe how to manage IPS services on Cisco IPS sensors and Cisco IOS IPS devices:

- [Understanding Network Sensing, page 13-2](#)
- [Configuring Interfaces, page 13-2](#)
- [Configuring Signatures, page 13-9](#)
- [Configuring Signature Settings, page 13-17](#)
- [Configuring Anomaly Detection, page 13-18](#)
- [Configuring Event Actions, page 13-21](#)
- [Configuring Policies Specific to IOS IPS Devices, page 13-24](#)

Understanding Network Sensing

Network sensing can be accomplished using Cisco IPS sensors (appliances, switch modules, network modules, and SSMs) and Cisco IOS IPS devices (Cisco IOS routers with IPS-enabled images and Cisco ISRs). These sensing platforms are components of the Cisco Intrusion Prevention System and can be managed and configured through 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 network flow validation, an extensive embedded signature library, and anomaly detection engines. However, these platforms differ in how they can respond to perceived intrusions.

**Note**

Cisco IPS sensors and Cisco IOS IPS devices are often referred to collectively as IPS devices or simply sensors.

When an IPS device detects unauthorized network activity, it can terminate the connection, permanently block the associated host, and take other actions. *Event actions* were previously called *alarms* in Cisco IPS.

Network sensing requires you to define several IPS policies. One of the most important policies is the tuning of an IPS device to achieve maximum security and optimal performance, and particularly to minimize false positives and false negatives. In Security Manager, the term used for tuning is editing signature parameters.

Configuring Interfaces

The Interfaces policy is where you configure interfaces for Cisco IPS sensors:

- [Configuring Physical Interfaces, page 13-4](#)
- [Configuring Bypass Mode, page 13-4](#)
- [Configuring Inline Pairs, page 13-5](#)
- [Configuring VLAN Pairs, page 13-6](#)
- [Configuring VLAN Groups, page 13-7](#)
- [Interface Summary, page 13-9](#)

**Note**

No interface configuration as described in this chapter is supported by Cisco IOS IPS.

Understanding Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface.

There are three interface roles: command and control, sensing, and alternate TCP reset. There are restrictions on which roles you can assign to specific interfaces, and some interfaces have more than one role. The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics. Sensing interfaces are used by the sensor to analyze traffic for security violations. Using alternate TCP reset interfaces, you can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host.

There are five interface modes: promiscuous (simple physical interface), inline interface mode, inline VLAN pair mode, physical interface VLAN group mode (IPS 6.0), and inline interface pair VLAN group mode (IPS 6.0). In promiscuous mode, packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. Operating in inline interface pair mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair. You can divide each physical interface or inline interface into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

Configuring Physical Interfaces

From the Interfaces policy, the Physical Interfaces tab lists the existing physical interfaces on your sensor and their associated settings. The sensor detects the interfaces and populates the summary table in the Physical Interfaces tab. In the Physical Interfaces policy, interfaces can only be edited; they cannot be added or deleted.

**Tip**

Each physical interface can be divided into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

To edit the physical interface settings, follow these steps:

-
- Step 1** In Device View, select the sensor whose physical interface settings you want to edit.
 - Step 2** Also in Device View, select **Interfaces > Physical Interfaces**.
 - Step 3** In the summary table on the Physical Interfaces tab, select the interface that you want to edit and click the **Edit** button. The Modify Physical Interface Map dialog box appears.
 - Step 4** You can change the description in the Description field, or change the state from enabled to disabled by selecting **Yes** or **No** in the list box. You can have the interface use the alternate TCP reset interface by checking the **Specify Interface for TCP Reset** check box.
 - Step 5** Click **OK**. The edited interface appears in the summary table in the Physical Interfaces tab.
 - Step 6** Click **Save** to apply your changes and save the revised configuration.
-

Configuring Bypass Mode

You can use inline bypass as a diagnostic tool and a failover protection mechanism. Normally, the sensor Analysis Engine performs packet analysis. When inline bypass is activated, Analysis Engine is bypassed, allowing traffic to flow through the inline interfaces and inline VLAN pairs without inspection.

Inline bypass ensures that packets continue to flow through the sensor when the sensor processes are temporarily stopped for upgrades or when the sensor monitoring processes fail. There are three modes: on, off, and auto(matic). By default, bypass mode is set to auto.

To change the bypass mode setting, follow these steps:

-
- Step 1** In Device View, select the sensor whose bypass mode settings you want to change.
 - Step 2** Also in Device View, select **Interfaces > Physical Interfaces**.
 - Step 3** Beneath the summary table on the Physical Interfaces tab, in the Bypass Mode field, select the mode that you want.
-

Configuring Inline Pairs

You can pair interfaces on your sensor if your sensor is capable of inline monitoring.

To configure inline pairs, follow these steps:

-
- Step 1** In Device View, select the sensor for which you want to pair interfaces.
 - Step 2** Also in Device View, select **Interfaces > Inline Pairs**.
 - Step 3** Click the **Add** button. The Add Interface Pair dialog box appears.
 - Step 4** Enter a name in the Interface Pair Name field. The inline interface name is a name that you assign.
 - Step 5** Select two interfaces to form a pair in the Interface A and Interface B fields. For example, select GigabitEthernet0/0 and GigabitEthernet0/1.
 - Step 6** You can add a description of the inline interface pair in the Description field if you want to.
 - Step 7** Click **OK**. The new inline pair appears in the summary table on the Inline Pairs tab.
 - Step 8** To edit an inline pair, select that pair and then click the **Edit** button. The Edit Interface Pair dialog box appears.

- Step 9** You can choose a new inline pair or edit the description. You cannot change the name.
 - Step 10** Click **OK**. The edited inline pair appears in the summary table on the Inline Pairs tab.
 - Step 11** To delete an inline pair, select that pair and then click the **Delete** button. The inline interface pair no longer appears in the summary table.
 - Step 12** Click **Save** to apply your changes and save the revised configuration.
-

Configuring VLAN Pairs

The summary table on the VLAN Pairs tab displays the existing VLAN pairs for each physical interface. Multiple VLAN pairs may be created on a single physical interface.

To configure a VLAN pair, follow these steps:

-
- Step 1** In Device View, select the sensor for which you want to configure a VLAN pair.
 - Step 2** Also in Device View, select **Interfaces > VLAN Pairs**.
 - Step 3** Click the **Add** button. The Add VLAN Pair dialog box appears.
 - Step 4** Choose an interface from the **Physical Interfaces** list box.
 - Step 5** Enter a subinterface number (1 to 255) for the VLAN pair in the Subinterface Number field.
 - Step 6** Specify the first VLAN (1 to 4095) for this VLAN pair in the VLAN A field.
 - Step 7** Specify the other VLAN (1 to 4095) for this VLAN pair in the VLAN B field.
 - Step 8** You can add a description of the inline VLAN pair in the Description field if you want to.
 - Step 9** Click **OK**. The new VLAN pair appears in the summary table on the VLAN Pairs tab.
 - Step 10** To edit an inline VLAN pair, select that pair and then click the **Edit** button. The Edit VLAN Pair dialog box appears.
 - Step 11** You can change the subinterface number, the VLAN numbers, or the description.
 - Step 12** Click **OK**. The edited VLAN pair appears in the summary table.

- Step 13** To delete a VLAN pair, select that pair and then click **Delete**. The VLAN pair no longer appears in the summary table.
- Step 14** Click **Save** to apply your changes and save the revised configuration.
-

Configuring VLAN Groups

Each physical interface can be divided into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface. Also, an inline interface can also be divided into VLAN group subinterfaces. More than one VLAN group can be created on a single physical interface or single inline pair, as long as each VLAN group is assigned a unique subinterface number.



Note

VLAN groups are supported in IPS 6.0 only.

A VLAN group consists of a group of VLAN IDs that exist on an interface. Each VLAN group consists of at least one VLAN ID. You can have up to 255 VLAN groups per interface (logical or physical). Each group can contain any number of VLAN IDs. You then assign each VLAN group to a virtual sensor (but not more than one virtual sensor). You can assign different VLAN groups on the same sensor to different virtual sensors. Certain IPS models support assignment of VLAN groups to a virtual sensor. The following sensors support assignment of promiscuous VLAN groups and inline VLAN groups to a virtual sensor: IDS-4235, IDS-4250-TX, IDS-4250-SX, IDS-4250-XL, IPS-4240, IPS-4255, and IPS-4260.

After you assign the VLAN IDs to the VLAN group, you must assign the VLAN group to a virtual sensor.

To configure a VLAN group, follow these steps:

- Step 1** In Device View, select the sensor for which you want to configure a VLAN group.
- Step 2** Also in Device View, select **Interfaces > VLAN Groups**.
- Step 3** Click **Add** to add a VLAN group. The Add VLAN Group Map dialog box appears.
- Step 4** In the Physical and Logical Interfaces list box, select an interface.

- Step 5** In the Subinterface Number field, enter a subinterface number (1 to 255) for the VLAN group.
- Step 6** Specify the VLAN group for this interface by selecting one of the following radio buttons:
- All Unassigned VLAN IDs**—Lets you assign all the VLANs that are not already specifically assigned to a subinterface.
 - Range of free VLAN IDs**—Lets you specify the VLANs that you want to assign to this subinterface. You can assign more than one VLAN (1 to 4095) in this pattern: 1, 5-8, 10-15. This lets you set up different policies based on VLAN ID. For example, you can make VLANs 1-10 go to one virtual sensor (VS0) and VLANs 20-30 go to another virtual sensor (VS1).



Note You need to have the VLAN IDs that are set up on your switch to enter in the Specify VLAN Group field.

- Step 7** You can add a description of the VLAN group in the Description field if you want to.
- Step 8** Click **OK**. The new VLAN group appears in the list in the VLAN Groups pane. You must assign this VLAN group to a virtual sensor.
- Step 9** To edit a VLAN group, select it, and click **Edit**. The Edit VLAN Group Map dialog box appears.
- Step 10** You can change the subinterface number, the VLAN group, or edit the description.
- Step 11** Click **OK**. The edited VLAN group appears in the summary table on the VLAN Groups tab.
- Step 12** To delete a VLAN group, select that group and then click **Delete**. The VLAN group no longer appears in the summary table.
- Step 13** Click **Save** to apply your changes and save the revised configuration.
-

Interface Summary

The Summary tab contains a table summarizing how you have configured the sensing interfaces—the interfaces you have configured for promiscuous mode, the interfaces you have configured as inline pairs, the interfaces you have configured as inline VLAN pairs, inline VLAN groups, and promiscuous VLAN groups. The content of this table changes when you change your interface configuration.

**Caution**

You can configure any single physical interface to run in promiscuous mode, inline pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

Configuring Signatures

The Signatures policy is where you configure signatures for Cisco IPS sensors:

- [Understanding Signatures, page 13-9](#)
- [Accessing the Cisco NSDB, page 13-10](#)
- [Understanding Signature Inheritance, page 13-11](#)
- [Editing Signatures—Severity, Fidelity Rating, and Action, page 13-12](#)
- [Enabling and Disabling Signatures, page 13-14](#)
- [Cloning Signatures, page 13-15](#)
- [Adding Custom Signatures, page 13-15](#)
- [Editing Signature Parameters \(Tuning Signatures\), page 13-16](#)

Understanding Signatures

Network intrusions are attacks on, or other misuses of, network resources. Cisco IPS sensors and Cisco IOS IPS devices use a signature-based technology to detect network intrusions. A signature specifies the types of network intrusions that you want the sensor to detect and report. As sensors scan network packets, they use signatures to detect known types of attacks, such as denial of service (DoS) attacks, and respond with actions that you define.

On a basic level, signature-based intrusion detection technology can be compared to virus-checking programs. Cisco IPS contains a set of signatures that the sensor compares with network activity. When a match is found, the sensor takes some action, such as logging the event or sending an alarm to the Cisco IPS Event Viewer (Cisco IEV).

Signatures can produce false positives, because certain normal network activity can be construed as malicious. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by editing your signature parameters (tuning your signatures).

Accessing the Cisco NSDB

The Cisco Network Security Database (NSDB) can be accessed, or invoked, through the user interface of Security Manager.

The NSDB is a database of security information that explains the signatures the IPS uses along with the vulnerabilities on which these signatures are based. The NSDB contains a description for each attack signature that the sensor can detect.

In Security Manager, the table in the content area of the IPS Signature policy contains several columns by default, one of which is Signature ID. The Signature ID column contains hyperlinks to the NSDB. Clicking on the link in the ID column will trigger the opening of an external browser window that opens to the entry in MySDN for that signature.

MySDN, which stands for My Self-Defending Network, provides up-to-date intelligence reports about current vulnerabilities and threats, as well as education on advanced security topics to help you protect your network, prioritize remediation, and structure your systems to reduce organizational risk. For more information, refer to <http://www.cisco.com/go/MySDN>.

If you have access to Cisco.com, then the signature ID is linked to MySDN. If you do not have access to Cisco.com, then the signature ID is linked to the local copy of the NSDB. Security Manager will detect whether or not you have access to Cisco.com and make the appropriate link for you without your having to set a preference.

Some signatures in IPS 5.x, IPS 6.0, and IOS IPS have special characteristics: Built-in signatures cannot be added, deleted, or renamed, because they are provided with IPS itself. (“Built-in” means all signatures other than those that you create.) The information for built-in signatures, such as their names and IDs, appears as it does in the NSDB. The other type of signatures, custom signatures, are those that you create. Custom signatures do not have MySDN links.

**Tip**

For a particular signature in the NSDB, the “Release Version” refers to the version of IPS that the signature first appeared in, or was last modified in. The “Release Version” appears in the bottom left-hand corner of the header information when you are looking at a particular signature.

Understanding Signature Inheritance

Signature inheritance for IPS devices is different than for any other Security Manager policy. Inheritance refers to the capability of Security Manager to enforce hierarchical lists of first-match, rule-based policies such as access rules. Signature inheritance is different because for IPS devices, Security Manager allows inheritance on a per-signature basis.

This example shows what is meant by inheritance on a per-signature basis:

-
- Step 1** In Policy View, select **IPS > Signatures > Signatures**.
 - Step 2** Create a policy named test1.
 - Step 3** Create a second policy, named test2.
 - Step 4** Right-click **test 2** and select **Inherit Signatures**. The Inherit Rules—test 2 dialog box appears.
 - Step 5** Select **test1** and click the **OK** button.
 - Step 6** Select **test1** and edit a signature. Note the edit that you made and save your change.
 - Step 7** Select **test2** and select the signature that you just edited. Observe that test2 inherited the editing that you did on test1.
-

Editing Signatures—Severity, Fidelity Rating, and Action

You can edit the following properties of Cisco IPS signatures:

- **Enable**—Configures the sensor to scan network traffic for that particular signature and to generate an alarm when an attack is detected. Disabling a signature causes the sensor to disregard any network traffic that displays the signature.
- **Retire**—Removes the signature from the signature micro-engine.



Note

You can enable a signature that is retired, but it then is not used to scan traffic, because it is not in the signature micro-engine. If you want a sensor to scan network traffic for a particular signature, you must enable it and not retire it.

- **Activate**—Changes the value in the Retired field from No to Yes
- **Sig Fidelity Rating (SFR)**—Identifies the weight associated with how well this signature might perform in the absence of specific knowledge of the target. This rating can be any number from 0 to 100, with 100 indicating the most confidence in the signature.
- **Severity**—Categorizes the attack. The severity setting is used in Event Viewer in Security Monitor to distinguish among the types of attacks being logged.
- **Action**—Determines the action or actions the sensor will take, in addition to generating an alarm, when it detects an attack. *Action* is the term in Cisco IPS 6.x for what previously was called *event action* or *alarm*. You can configure a variety of actions to add or remove activities associated with a signature event.
- **Signature Name**—Used when adding a new signature (not used for all categories and groupings of signatures).

You cannot edit the following properties of signatures:

- **Signature ID**—The ID of the signature, which is generated by Security Manager (generated only for custom signatures).
- **Subsig ID**—Specifies the subsignature ID (not used for all signatures). For example, every string-matching signature has a subsignature ID, which is generated by Security Manager. Also, every ACL violation signature has a

subsignature ID, which is generated by Security Manager. When you create an ACL violation signature, the Subsig ID field is populated with a value that is greater by 1 than the subsignature having the highest number in the list.

Some signatures have special characteristics:

- Build-in signatures cannot be added, deleted, or renamed, because they are provided with the sensor software.

The information for built-in signatures, such as their names and IDs, reflects how it is recorded in the Cisco Network Security Database (NSDB). To view the NSDB from the Signatures page, click a signature ID, such as 2000, in the ID column. The entries in the ID column are hyperlinks to the NSDB.

- No custom signatures are provided with a new 5.x or 6.x sensor. You can create custom signatures and modify any existing custom signatures. However, you cannot create a custom signature that has the same ID as another custom signature.

Some signatures have special requirements. For example, to configure a sensor to detect ACL violation signatures, you must first configure one or more Cisco IOS routers to log ACL violations. Then, you must configure those routers to communicate with the sensor. Finally, you must configure the sensor to accept syslog traffic from those routers.

To edit a signature, follow these steps:

Step 1 In Device View, select the sensor whose signature you want to edit.

Step 2 Also in Device View, select **IPS > Signatures > Signatures**. The signature summary table appears.



Tip You can filter the display of the signature table. Using the Filter list, select any of the displayed columns as the filter source. Next, enter a value in the adjacent field and click **Apply**. For example, select **Severity** in the list box and enter the value High in the adjacent field. When you click **Apply**, the signature table displays all signatures that have a high severity. Click **Clear** to cancel filtering.

Step 3 In the summary table on the Signatures page, find the signature that you want to edit and right-click its row. The row shortcut menu appears.

Step 4 In the row shortcut menu, click **Edit Row**. The Edit Signature dialog box appears.



Note The default policy cannot be edited, so if you want to change the signature settings, you will have to override them in the local policy for the device. You can do this by selecting Local from the Source Policy list box. After you change the source policy to Local, the controls are enabled.

- Step 5** Edit the Severity, Fidelity, or Actions by selecting a new value in those fields.
- Step 6** Click **OK**. The edited signature property appears in the summary table on the Signatures page.
- Step 7** Click **Save** to apply your changes and save the revised configuration.
-

Enabling and Disabling Signatures

To enable or disable a signature, follow these steps:

- Step 1** In Device View, select the sensor whose signature you want to enable or disable.
- Step 2** Also in Device View, select **IPS > Signatures > Signatures**.
- Step 3** In the summary table on the Signatures page, find the signature that you want to enable or disable and right-click its row. The row shortcut menu appears.
- Step 4** In the row shortcut menu, click **Enable** or **Disable**. The signature appears enabled or disabled in the summary table on the Signatures page.
- Step 5** Click **Save** to apply your changes and save the revised configuration.
-

Cloning Signatures

To clone a signature, follow these steps:

- Step 1** In Device View, select the sensor whose signature you want to clone.
- Step 2** Also in Device View, select **IPS > Signatures > Signatures**.

- Step 3** In the summary table on the Signatures page, find the signature that you want to clone and right-click its row. The row shortcut menu appears.
- Step 4** In the row shortcut menu, click **Clone**. The Add Custom Signature dialog box appears.
- Step 5** Edit the properties of the clone.
- Step 6** Click **OK**. The clone appears in the summary table on the Signatures page.
- Step 7** Click **Save** to apply your changes and save the clone.

**Note**

Cloned signatures are enabled and active by default.

Adding Custom Signatures

To add a custom signature, follow these steps:

-
- Step 1** In Device View, select the sensor for which you want to add a custom signature.
- Step 2** Also in Device View, select **IPS > Signatures > Signatures**.
- Step 3** In the summary table on the Signatures page, right-click on a row (any row). The row shortcut menu appears.
- Step 4** In the row shortcut menu, click **Add Row**. The Add Custom Signature dialog box appears.

**Timesaver**

In place of steps 3 and 4, you can click the **Add** button at the bottom of the table.

- Step 5** Click the **Edit Parameters** button. The Edit Signature Parameters dialog box appears. At a minimum, you must click the **OK button** on the Edit Signature Parameters dialog box; you do not need to edit any parameters, but if you click the **Cancel** button first, your custom signature will not be created.
- Step 6** Click **OK**. The custom signature appears in the summary table on the Signatures page.
- Step 7** Click **Save** to apply your changes and save the clone.

**Note**

Custom signatures are enabled and active by default.

Editing Signature Parameters (Tuning Signatures)

After you configure your sensors, you must edit their parameters (tune them) to achieve optimal performance on your network, and particularly to minimize false positives and false negatives.

A *false positive* occurs when legitimate network activity, such as virus scanning, is interpreted and reported as an attack. This happens when network activity meets criteria that were specified to identify an attack before the attack occurred. You can decrease the number false positives by tuning your sensor configurations.

A *false negative* occurs when an attack was not detected. Tuning your sensor configurations will help you decrease the number of false negatives.

This procedure describes how to edit signature parameters (tune a signature).

Procedure

- Step 1** In Device view, select an IPS device from the Device selector.
 - Step 2** Also in Device view, select **IPS > Signatures > Signatures**.
 - Step 3** In the summary table on the Signatures page, find the signature whose parameters you want to edit and right-click its row. The row shortcut menu appears.
 - Step 4** Click **Edit Row**. The Edit Signature dialog box appears.
 - Step 5** In the Source Policy Field, change the setting to Local to enable editing.
 - Step 6** Click **Edit Parameters**. The Edit Signature Parameters dialog box appears.
 - Step 7** In the category you want, such as Engine, select the setting you want, such as Fragment Status, and then select a value from among those available, such as Fragmented.
 - Step 8** Click the **OK** button to save your changes.
-

Configuring Signature Settings

The Settings page is where you configure signature settings for Cisco IPS sensors that define application policy (enable HTTP, maximum number of HTTP Requests, AIC web ports, and enable FTP), fragment reassembly policy, stream reassembly policy, and IP logging policy. These settings result in policies that can be shared but cannot be inherited. When a new IPS device is added, it has a local policy that contains the default settings for all signatures.

Signature settings policies are supported with these features:

- Enable HTTP
- Max HTTP Requests
- AIC Web Ports
- Enable FTP
- IP Reassembly Mode
- TCP Handshake Required
- TCP Reassembly Mode
- Max IP Log Packets
- IP Log Time
- Max IP Log Bytes

Configuring signature settings consists of four tasks:

-
- Step 1** **Define application policy.** Enable or disable HTTP, determine and specify the maximum number of HTTP requests, specify AIC web ports, and enable or disable FTP. For detailed descriptions of these settings, see [Table N-20 on page N-33](#).
- Step 2** **Define fragment reassembly policy.** Configure the sensor to reassemble a datagram that has been fragmented over more than one packet by selecting the IP reassembly mode. For a detailed descriptions of the IP reassembly mode, see [Table N-20 on page N-33](#).

- Step 3 Define stream reassembly policy.** Configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake by specifying whether or not a TCP handshake is required and by selecting the TCP reassembly mode. For detailed descriptions of these settings, see [Table N-20 on page N-33](#).
- Step 4 Define IP logging policy.** Configure the sensor to generate an IP session log when the sensor detects an attack by determining and selecting the maximum allowable number of log packets, the IP log time and the maximum allowable size of the IP log. For detailed descriptions of these settings, see [Table N-20 on page N-33](#).
-

Configuring Anomaly Detection

Anomaly detection is a new feature, introduced with Cisco IPS 6.x sensors. Not all Cisco IPS devices support anomaly detection.

Anomaly detection is designed to recognize network congestion caused by worm traffic that exhibits scanning behavior. Anomaly detection also will identify infected hosts on the network that are scanning for other vulnerable hosts.

**Note**

Anomaly detection is not supported by Cisco IOS IPS.

Explaining Anomaly Detection

The anomaly detection component of the sensor detects worm-infected hosts that exhibit scanning-type behavior. This enables the sensor to be less dependant on signature updates for protection again worm viruses, such as Code-red and SQL-slammer and so forth. The anomaly detection component lets the sensor learn normal activity and then sends alerts and takes dynamic response actions for behavior that deviates from what it has learned as normal behavior.

**Note**

Anomaly detection does not detect email-based worms, such as Nimda.

Anomaly detection recognizes when a single or multiple worm-infected source starts scanning for other vulnerable hosts.

Worm Viruses

Worm viruses are automated, self-propagating, intrusion agents that make copies of themselves and then facilitate their spread. Worm viruses attack a vulnerable host, infect it, and then use it as a base to attack other vulnerable hosts. They search for other hosts by using a form of network inspection, typically a scan, and then propagate to the next target. A scanning worm virus locates vulnerable hosts by generating a list of IP addresses to probe, and then contacts the hosts. Code Red worm, Sasser worm, Blaster worm, and the Slammer worm are examples of worms that spread in this manner.

Anomaly detection identifies worm-infected hosts by their behavior as a scanner. To spread, a worm virus must find new hosts. It finds them by scanning the Internet using TCP, UDP, and other protocols to generate unsuccessful attempts to access different destination IP addresses. A scanner is defined as a source IP address that generates events on the same destination port (in TCP and UDP) for too many unresponsive destination IP addresses.

The events that are important for TCP protocol are non-established connections, such as a SYN packet that does not have its SYN-ACK response for a given amount of time. A worm-infected host that scans using TCP protocol generates non-established connections on the same destination port for an anomalous number of IP addresses.

The events that are important for UDP protocol are unidirectional connections, such as a UDP connection where all packets are going in only one direction. A worm-infected host that scans using UDP protocol generates UDP packets but does not receive UDP packets on the same quad within a time-out period on the same destination port for multiple destination IP addresses.

The events that are important for other protocols, such as ICMP, are from a source IP address to many different destination IP addresses, that is, packets that are received in only one direction.



Caution

If a worm virus has a list of IP addresses it should infect and does not have to use scanning to spread itself (for example, it uses passive mapping—listening to the network as opposed to active scanning), it will not be detected by anomaly

detection's worm policies. Worm viruses that receive a mailing list from probing files within the infected host and email this list will not be detected, because no L3/L4 anomaly is generated.

Learning Mode

Anomaly detection initially conducts a “peacetime” learning process when the most normal state of the network is reflected. Anomaly detection then derives a set of policy thresholds that best fit the normal network. This is done in two phases:

- **Initial setup**—In the initial setup, the sensor is in learning mode. We assume that during this phase no attack is being carried out. Anomaly detection creates an initial baseline, known as a knowledge base, of the network traffic. The default amount of time for anomaly detection to be in learning mode is 24 hours, but depending on your network complexity, you may want to change the default. After the learning mode time has expired, you terminate this phase by configuring anomaly detection to operate in detect mode.
- **Ongoing operation**—For ongoing operation, the sensor is in learning plus detecting mode. This is for 24 hours, 7 days a week. Once a knowledge base has been created, anomaly detection detects attacks based on it. It looks at the network traffic flows that violate thresholds in the knowledge base and send alerts. As anomaly detection looks for anomalies, it also records gradual changes to the knowledge base that do not violate the thresholds and thus creates a new knowledge base. The new knowledge base is periodically saved and takes the place of the old one thus maintaining an up-to-date knowledge base.

By default, anomaly detection functions even if you do not follow the two phases and manually change the operational mode from learning to detect. Anomaly detection does not detect attacks when working with the initial knowledge base, which is empty. After the default of 24 hours, the default operational mode is changed to detect. A knowledge base is saved and loaded and now anomaly detection also detects attacks.

Anomaly Detection Zones

By subdividing the network into zones, you can achieve a lower false negative rate. A zone is a set of destination IP addresses. There are three zones, each with its own thresholds: internal, illegal, and external.

The external zone is the default zone with the default Internet range of 0.0.0.0-255.255.255.255. By default, the internal and illegal zones contain no IP addresses. Packets that do not match the set of IP addresses in the internal or illegal zone are handled by the external zone.

We recommend that you configure the internal zone with the IP address range of your internal network. If you configure it in this way, the internal zone is all the traffic that comes to your IP address range, and the external zone is all the traffic that goes to the Internet.

You can configure the illegal zone with IP address ranges that should never be seen in normal traffic, for example, unallocated IP addresses or part of your internal IP address range that is unoccupied. An illegal zone can be very helpful for accurate detection, because we do not expect any legal traffic to reach this zone. This allows very low thresholds, which in turn can lead to very quick worm virus detection.

Configuring Event Actions

An event is an IPS message that contains an alert, a block request, a status message, or an error message. An event action is the sensor's response to an event. An event action happens only if the event is not filtered. Possible event actions are TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet. Event actions were known as alarms in Cisco IPS versions earlier than 5.x.

The Event Actions folder is where you configure settings for the event action processing component of the sensor. These settings define the actions for the sensor to take when an event is detected:

- [Configuring Event Action Filters, page 13-22](#)
- [Configuring Event Action Overrides, page 13-22](#)
- [Configuring Network Information, page 13-22](#)
- [Configuring Settings for Event Actions, page 13-24](#)

Configuring Event Action Filters

A Cisco IPS 5.x or 6.x EAF removes one or more actions from the signature event. For any given signature event, the filters are applied in the order specified in the summary table. EAFs are listed as either default or mandatory.

An EAF removes one or more actions from the signature event. For a given signature event, filters are applied in the order specified in the Signature Event Action Filters summary table. EAFs are processed on a first-match basis. You can move filters up or down in the summary table to change the order of their application.

You can define filters on the basis of signature categories such as operating system signatures and web signatures.

Configuring Event Action Overrides

Event action overrides (EAOs) add actions to the signature event, based on some criteria. You configure the following configuration elements when adding an EAO:

- **Signature Event Action**—A selection from the list of signature event actions.
- **Risk Rating Inclusive Range (0-100)**—The range of RR values at which the EAO is valid. This is expressed as two numbers, each from 0 to 100, separated by a hyphen. For example, 0-66.
- **Enable action**—A check box that when selected enables EAO.

Configuring Network Information

The Network Information Page is where you configure Target Value Ratings and OS Identification (Cisco IPS 6.x sensors only).

**Note**

OS Identification is not supported by Cisco IPS 5.x sensors or by IOS IPS.

Understanding Target Value Ratings

A target value rating (TVR) is one weight factor that is used to calculate the Risk Rating (RR) value for each alert. You can assign different TVR values to different targets based on the importance of the target. You have the following choices for TVR values: No value, Low, Medium, High and Mission Critical. You can configure TVRs at the device, group, or global levels. The addresses you specify in the TVR are one of the following possible choices: a single IP address, a range of IP addresses, or a variable.

Configuring Target Value Ratings

The Target Value Ratings tab on the Network Information page is where you configure TVRs for 5.x sensors and 6.x sensors. The addresses you specify in the TVR are one of the following possible choices: a single IP address, an IP address range, a set of IP address ranges, a building blocks.

When you add a TVR you specify its type, a value that corresponds to that type, and value rating. The following configuration elements and corresponding values apply:

- **Variable**—The name of a variable.
- **Single IP**—An IP address in standard form.
- **Range**—The Start IP Address and the End IP Address, both in standard form.
- **Value Rating**—One of the following: Low, Medium, High, Mission Critical.

Configuring OS Identification (Cisco IPS 6.x Sensors Only)

The OS Identification (6.x only) tab on the Network Information page is where you configure passive OS fingerprinting for 6.x sensors.

**Note**

OS Identification is not supported by Cisco IPS 5.x sensors or by IOS IPS.

Passive OS fingerprinting functions as part of the sensor. As the sensor analyzes network traffic between hosts, the sensor stores the identity of the OS running on the hosts alongside the IP addresses of the hosts. The sensor determines the identity of the OSs on the hosts by inspecting characteristics of the packets

exchanged on the network. The sensor then uses the target system's OS information to compute the ARR (Attack Relevance Rating) component for RR (Risk Rating). The RR can then be used to drop suspicious packets.

Configuring Settings for Event Actions

The Settings Page in the Event Actions folder is where you configure the following settings:

- Enable Event Action Overrides
- Enable Event Action Filters
- Enable Event Action Summarizer
- Enable Meta Event Generator
- Enable Threat Rating Adjustment
- Deny Attacker Duration in Seconds
- Block Action Duration in minutes
- Maximum number of Denied Attackers

For detailed information on these settings, see [Event Actions > Settings Page, page N-60](#).

Configuring Policies Specific to IOS IPS Devices

This section details policies that are specific to IOS IPS devices supported by Security Manager:

- [Understanding Cisco IOS IPS, page 13-25](#)
- [Limitations and Restrictions, page 13-25](#)
- [Preparation for Use, page 13-26](#)
- [Signatures, page 13-26](#)
- [General Settings, page 13-27](#)
- [Interface Rules, page 13-27](#)

Understanding Cisco IOS IPS

You can use Cisco Security Manager with the Cisco IOS Intrusion Prevention System (IOS IPS) to manage intrusion prevention on Cisco routers that use supported Cisco IOS releases.

The earliest support by Cisco Security Manager 3.1 for IOS IPS is in IOS 12.4(11)T2.



The IPS subsystem version is a version number used to keep track of Cisco IOS IPS feature changes. You can use the command `show subsys name ips` at a command line on the router that is running Cisco IOS IPS to show the detailed Cisco IOS IPS subsystem version.

Cisco IOS IPS acts as an inline, signature-based IPS sensor that can be turned on in Cisco IOS Software router platforms with security feature images. Cisco IOS IPS can be configured to respond to signature identification by dropping packets, resetting connections, and sending alarms. Within Security Manager you can configure policies specific to IOS IPS, such as editing, deleting, enabling, and disabling signatures in addition to configuring event actions.

Limitations and Restrictions

Cisco IOS IPS devices (Cisco IOS routers with IPS-enabled images and Cisco Integrated Services Routers [ISRs]) do not support all the features that are supported by IPS sensors (appliances, switch modules, network modules, and Security Service modules [SSMs]). In addition, routers that support IOS IPS may not allocate as much memory to IPS functionality as an IPS sensor does. The following limitations and restrictions are important:

- When configuring an IOS IPS device, select only the signatures that you need. If you select all signatures that are available in Security Manager, the IOS IPS device may fail from loading the signatures or performance may be significantly degraded.
- Anomaly detection is not supported by Cisco IOS IPS.
- OS Identification is not supported by IOS IPS.
- Virtual sensors are not supported by IOS IPS.

- When using event action filters with an IOS IPS device, only a subset of IPS actions are available for removal from an event that meets the criteria of the event action filter. For detailed information, see [Filter Item Dialog Box, page N-49](#).

Preparation for Use

You must prepare an IOS router before you can use it as an IOS IPS device. Preparation for use consists of the following steps:

-
- Step 1** Download Cisco IOS IPS Files.
 - Step 2** Create a Directory on Flash.
 - Step 3** Configure a Cisco IOS IPS Crypto Key.
 - Step 4** Enable Cisco IOS IPS. Also enable HTTP/HTTPS, without which discovery fails.
 - Step 5** Load Signatures to Cisco IOS IPS.
-

For detailed procedures, see [Getting Started with Cisco IOS IPS with 5.x Format Signatures](#).

Signatures

You can use Security Manager to configure IOS IPS signature policies such as editing, deleting, enabling, and disabling signatures. You can also create custom signatures.

Signature Sets in Previous Versions of IOS IPS

Built-in signatures are removed from Cisco IOS IPS starting from Cisco IOS Software Release 12.4(11)T. In previous releases, built-in signatures are predefined signatures bundled with Cisco IOS Software. These built-in signatures exist solely to maintain backward compatibility with the previous Cisco IOS Intrusion Detection System (IDS), which has about 135 signatures. Cisco does not recommend using built-in signatures.

The basic signature set (in file 128MB.sdf) and the advanced signature set (in file 256MB.sdf) are not used by Security Manager 3.1.

Cisco decommissioned the use of the file attack-drop.sdf.

General Settings

The General Settings page is where you specify the global settings used for IPS rules defined for a particular router. Security Manager enables you to configure two general settings for IOS IPS devices:

- Traffic Blocking when IPS engine unavailable setting
- Deny Action Properties
- SDEE Properties
- IPS Config Location properties

Configuring general settings consists of four tasks:

-
- | | |
|---------------|---|
| Step 1 | Determine whether or not all traffic should be denied if the IPS engine is unavailable. For detailed information on this setting, see General Settings Page, page N-104 . |
| Step 2 | Determine whether to cause Cisco IPS to apply the ACLs directly to the Cisco IPS interfaces, rather than to the interfaces that originally received the attack traffic. For detailed information on this setting, see General Settings Page, page N-104 . |
| Step 3 | Configure SDEE properties. For detailed information on this setting, see General Settings Page, page N-104 . |
| Step 4 | Configure IPS Config Location properties. For detailed information on this setting, see General Settings Page, page N-104 . |
-

Interface Rules

Cisco IPS rules specify the interface or interfaces and the direction of traffic relative to the interface(s) that Cisco IPS is to examine. Additionally, the interface rule may also define a sub-set of the IP traffic to be examined, by assigning an ACL to select or filter IP traffic.

The Interface Rules page is where you add and edit IPS rules for Cisco IOS IPS devices. For detailed information on adding and editing IPS rules, see [Interface Rules Page, page N-107](#).